SOME FINITENESS RESULTS ON MONOGENIC ORDERS IN POSITIVE CHARACTERISTIC

JASON P. BELL AND KHOA D. NGUYEN

Abstract. This work is motivated by the papers [EG85] and [Ngu15] in which the following two problems are solved. Let $\mathcal{O}$ be a finitely generated $\mathbb{Z}$-algebra that is an integrally closed domain of characteristic zero, consider the following problems:

(A) Fix s that is integral over $\mathcal{O}$, describe all t such that $\mathcal{O}[s] = \mathcal{O}[t]$.
(B) Fix s and t that are integral over $\mathcal{O}$, describe all pairs $(m, n) \in \mathbb{N}^2$ such that $\mathcal{O}[s^m] = \mathcal{O}[t^n]$.

In this paper, we solve these problems and provide a uniform bound for a certain "discriminant form equation" that is closely related to Problem (A) when $\mathcal{O}$ *has characteristic* $p > 0$. While our general strategy roughly follows [EG85] and [Ngu15], many new delicate issues arise due to the presence of the Frobenius automorphism $x \mapsto x^p$. Recent advances in unit equations over fields of positive characteristic together with classical results in characteristic zero play an important role in this paper.

1. Introduction

Throughout this paper, let $\mathbb{N}$ denote the set of positive integers, let $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, and let p be a prime number. For every power $q > 1$ of p, let $\mathbb{F}_q$ denote the finite field of order q.

Let $\mathcal{O}$ be a finitely generated $\mathbb{Z}$-algebra that is an integrally closed domain with fraction field K. Rings of the form $\mathcal{O}[s]$ where s is integral over $\mathcal{O}$ and separable over K are called *monogenic orders* over $\mathcal{O}$. When $\mathrm{char}(\mathcal{O}) = 0$, certain diophantine aspects of monogenic orders over $\mathcal{O}$ have been studied extensively by Győry, Evertse and other authors [Győ84], [EG85], [BH09], [BEG13], [Ngu15]. More specifically, when $\mathrm{char}(\mathcal{O}) = 0$, the following two problems are solved in [Győ84], [EG85], [BH09], and [Ngu15]:

(A) Fix s that is integral over $\mathcal{O}$ and separable over K, describe all t such that $\mathcal{O}[s] = \mathcal{O}[t]$.
(B) Fix s and t that are integral over $\mathcal{O}$ and separable over K, describe all pairs $(m, n) \in \mathbb{N}^2$ such that $\mathcal{O}[s^m] = \mathcal{O}[t^n]$.

For Problem (A), Győry [Győ84] and Evertse-Győry [EG85] prove that there are finitely many elements $t_1, \ldots, t_N$ such that $\mathcal{O}[t_i] = \mathcal{O}[s]$ for $1 \le i \le N$, and if $\mathcal{O}[t] = \mathcal{O}[s]$ then $t = at_j + b$ for some $1 \le j \le N$, $a \in \mathcal{O}^*$, and $b \in \mathcal{O}$. Moreover, there is a remarkable uniform bound on N. After that, Bell and Hare [BH09], [BH12] study Problem (A) and a weak form of Problem (B) in the special case when $\mathcal{O} = \mathbb{Z}$

Date: August 30, 2015.
2010 *Mathematics Subject Classification.* Primary: 11D61; Secondary: 11R99, 11T99.
Key words and phrases. positive characteristic, unit equations, discriminant equations, monogenic orders.

and s and t are algebraic integers satisfying certain properties. The main motivation for their work is the so called Pisot-cyclotomic numbers which have applications in the study of quasicrystals and quasilattices. Finally, in [Ngu15, Theorem 1.4], the second author settles Problem (B) by proving that outside certain explicit "degenerate" families, there are only finitely many $(m, n) \in \mathbb{N}^2$ such that $\mathcal{O}[s^m] = \mathcal{O}[t^n]$. Broadly speaking, all of these papers use the fact that a linear equation has only finitely many non-degenerate solutions taken inside a finitely generated group. Such unit equations play a very important role in classical diophantine geometry (see, for instance, [ESS02], [BG06, Chapter 5], and [EG15]).

The question of what happens when $\mathrm{char}(\mathcal{O}) = p$ is natural and interesting on its own. It is well-known that a naïve analogue in characteristic p of many fundamental diophantine problems in characteristic 0 does not hold and, sometimes, formulating a correct statement is as important as the proof itself. One of the most spectacular examples is a positive characteristic analogue of the celebrated Mordell-Lang Conjecture for semi-abelian varieties [AV92] proved by Hrushovski [Hru96]. Certain aspects of Hrushovski's work have been refined by results of Moosa-Scanlon [MS04] and Ghioca [Ghi08]. When the ambient semi-abelian variety is a torus, the resulting intersection in the Mordell-Lang Conjecture corresponds to solutions of certain unit equations taken inside a finitely generated group. Thanks to further work of Voloch, Masser, Derksen, Adamczewski, and the first author [Vol98], [Mas04], [Der07], [AB12], [DM12], rather complete results on such unit equations (in characteristic p) have been obtained.

For the rest of this paper, assume $\mathrm{char}(\mathcal{O}) = p$ *and* K *has transcendence degree at least one over* $\mathbb{F}_p$. Note that the case $K \subset \bar{\mathbb{F}}_p$ renders both problems (A) and (B) obvious. While our approach to these problems roughly follows the general strategy in [Győ84], [EG85], and [Ngu15], new delicate algebraic and combinatorial issues arise due to the presence of the Frobenius automorphism $x \mapsto x^p$. For Problem (A), at first glance, we might modify the results of Evertse-Győry by asking if there exist finitely many elements $t_1, \ldots, t_N$ such that every t with $\mathcal{O}[t] = \mathcal{O}[s]$ has the form $t = at_i^{p^m} + b$ for some $1 \leq i \leq N$, $m \in \mathbb{N}_0$, $a \in \mathcal{O}^*$, and $b \in \mathcal{O}$. However, this is not true and a slight modification is needed as illustrated in the next example:

Example 1.1. Let $\mathcal{O} = \mathbb{F}_2[x]$ and let y be a root of $Y^4 + x^2Y^2 + Y + 1 = 0$. Let $s = xy$. For every $m \in \mathbb{N}_0$, write $s_m = xy^{4^m}$. It is not difficult to show that s_m and s have the same discriminant over K and $s_{m+1} \in \mathcal{O}[s_m]$ for every $m \in \mathbb{N}_0$ (see Subsection 3.3, especially the proof of Lemma 3.10), we have that $\mathcal{O}[s_m] = \mathcal{O}[s]$ for every m. It is not hard to check that for $i \neq j$, the element s_i does not have the form $as_j^{2^m} + b$ for some $a \in \mathcal{O}^* = \{1\}$ and $b \in \mathcal{O}$. On the other hand, we can describe the collection $(s_i)_{i \geq 0}$ by:

$$s_i = u_i s^{4^i}$$

where the collection $(u_i = x^{1-4^i})_{i \geq 0}$ consists of certain powers of the element x. A similar and more complicated example will be given in Subsection 3.3.

This example shows that, in a certain qualitative sense, our result below on Problem (A) is optimal (also see Remark 1.3). Similar to results by Evertse-Győry [EG85], our bound depends uniformly on (certain invariants of) the ring $\mathcal{O}$ and the degree $[K(s) : K]$ as follows. By a theorem of Roquette [Roq58], the unit group $\mathcal{O}^*$ is finitely generated. Let $q(K)$ be the power of p such that $K \cap \bar{\mathbb{F}}_p = \mathbb{F}_{q(K)}$, hence

$|\mathcal{O}^*_{\text{tors}}| = q(K)-1$. Let $V = \text{Spec}(\mathcal{O})$ and fix a choice of a projective normal scheme $\bar{V}$ over $\mathbb{F}_{q(K)}$ together with an open embedding from V to $\bar{V}$. Let M_K be the set of discrete valuations on K associated to the Weil divisors of $\bar{V}$ (see [Har77, pp. 130]) and let S be the finite subset of M_K corresponding to the Weil divisors contained in $\bar{V} \setminus V$. For $v \in M_K$, let n_v denote the degree of the Weil divisor corresponding v (see [Har77]). We have the following properties:

(i) For every $a \in K^*$, $v(a) = 0$ for all but finitely many $v \in M_K$ and $\sum_{v \in M_K} n_v v(a) = 0$ (base change from $\mathbb{F}_{q(K)}$ to $\bar{\mathbb{F}}_p$ and use [Har77, Exercise II.6.2(d)]).
(ii) $\mathcal{O} = \{a \in K : \ v(a) \geq 0 \text{ for every } v \in M_K \setminus S\}$ (see [Har77, pp. 132]).
(iii) $\mathbb{F}^*_{q(K)} = \{a \in K^* : v(a) = 0 \text{ for every } v \in M_K\}$ (see [Har77, pp. 122]).

For every element α that is separable over K, we define the discriminant of α over K by:

$$\text{discr}_K(\alpha) = \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)^2$$

where $\alpha_1, \ldots, \alpha_d$ are all the conjugates of α over K. Our first main result provides an answer to Problem (A) with a uniform bound on $q(K)$, $|S|$, and $[K(s) : K]$:

Theorem 1.2. *Let s be integral over $\mathcal{O}$ and separable over K of degree $d = [K(s) : K] \geq 2$ and let $D = \text{discr}_K(s)$. There are*

$$N \leq q(K)^{d^6} + \left(\exp(18^{10}) p^{3d^4|S|} \log_p q(K)\right)^{d^3}$$

elements $t_1, \ldots, t_N$ satisfying the following conditions:

(a) *$\mathcal{O}[t_i] = \mathcal{O}[s]$ for $1 \leq i \leq N$.*
(b) *If $\mathcal{O}[t] = \mathcal{O}[s]$ then $t = at_i^q + b$ where $1 \leq i \leq N$, $q \geq 1$ is a power of p, $a, b \in K$ such that $\dfrac{a^{d(d-1)}}{D^{1-q}} \in \mathcal{O}^*$.*

Remark 1.3. We will prove a slightly more precise result, see Theorem 3.3 and Remark 3.4. In characteristic zero, we have the form $t = at_i + b$ instead of part (b) (see [EG85] or [Ngu15, pp. 6–9]) with $a \in \mathcal{O}^*$ and, hence, b must automatically be in $\mathcal{O}$. On the other hand, we will construct an example in Subsection 3.3 to show that in characteristic p, it is not always possible to have $t = at_i^q + b$ as in Theorem 1.2 with the further restriction that b is in $\mathcal{O}$.

It is well-known that the "monogenic order equation" $\mathcal{O}[t] = \mathcal{O}[s]$ is closely related to the problem of solving for integral elements with a given discriminant (see, for example, [Győ84] and [EG85]). Now for the equation $\text{discr}_K(t) = \delta$ with a given δ, we may consider a more general problem by defining $\tilde{\mathcal{O}} = \mathcal{O}[1/\delta]$ and solving for t that is integral over $\tilde{\mathcal{O}}$ with $\text{discr}_K(t) \in \tilde{\mathcal{O}}^*$. This motivates our next result.

For a finite subset $T \subset M_K$ containing S, the set of T-integral elements of K is defined to be:

$$\mathcal{O}_{K,T} := \{a \in K : v(a) \geq 0 \text{ for every } v \in M_K \setminus T\}.$$

In particular $\mathcal{O}_{K,S} = \mathcal{O}$. Theorem 1.2 immediately gives the following:

Corollary 1.4. *Let E be a separable extension of degree d over K and let T be a finite subset of M_K containing S. Let $N(d)$ denote the number of subgroups of the symmetric group* $\mathrm{Sym}(d)$*. Then there are*

$$N \leq N(d)\left(q(K)^{d^6} + \left(\exp(18^{10})p^{3d^4|T|}\log_p q(K)\right)^{d^3}\right)$$

elements $t_1, \ldots, t_N$ in E satisfying the following conditions:

(a) *For $1 \leq i \leq N$, t_i is integral over $\mathcal{O}_{K,T}$ and $\mathrm{discr}_K(t_i) \in \mathcal{O}_{K,T}^*$.*
(b) *If $t \in E$ is integral over $\mathcal{O}_{K,T}$ and $\mathrm{discr}_K(t) \in \mathcal{O}_{K,T}^*$ then $t = at_i^q + b$ where $1 \leq i \leq N$, $q \geq 1$ is a power of p, $a \in \mathcal{O}_{K,T}^*$, and $b \in \mathcal{O}_{K,T}$.*

Remark 1.5. If $\mathrm{discr}_K(t_i) \in \mathcal{O}_{K,T}^*$ and $t = at_i^q + b$ as above then $\mathrm{discr}_K(t) \in \mathcal{O}_{K,T}^*$. Therefore Corollary 1.4 is optimal (at least qualitatively).

We now address Problem (B) where similar issues arise due to the Frobenius automorphisms. Note that when $\mathrm{char}(\mathcal{O}) = 0$, the main result of [Ngu15, Theorem 1.3] implies that the set $\{(m,n) : \mathcal{O}[s^m] = \mathcal{O}[t^n]\}$ is the union of a finite set and at most finitely many "progressions" of the form $\{(km_0, kn_0) : k \in \mathbb{N}\}$ for some (m_0, n_0). However, when $\mathrm{char}(\mathcal{O}) = p$, if $\mathcal{O}[s^m] = \mathcal{O}[t^n]$ then $\mathcal{O}[s^{pm}] = \mathcal{O}[t^{pn}]$; therefore infinite sets of the form $\{(p^k m_0, p^k n_0) : k \in \mathbb{N}_0\}$ will arise. We now give further examples that more complicated sets could appear.

For s and t that are integral over $\mathcal{O}$ and separable over K, we denote:

$$\mathcal{M}(\mathcal{O}, s, t) := \{(m,n) \in \mathbb{N}^2 : \mathcal{O}[s^m] = \mathcal{O}[t^n]\}.$$

Example 1.6. Suppose for some $(m_0, n_0) \in \mathbb{N}^2$ and some power $q > 1$ of p, we have $\mathcal{O}[s^{m_0}] = \mathcal{O}[t^{n_0}] = \mathcal{O}[t^{qn_0}]$. Then we have:

$$\{(q^i m_0, q^j n_0) : i, j \in \mathbb{N}_0\} \subseteq \mathcal{M}(\mathcal{O}, s, t).$$

Example 1.7. Here is an explicit example where a set of the form

$$\{(c_1 q^i + c_2 q^j, c_3 q^i + c_4 q^j) : i, j \in \mathbb{N}_0\}$$

for some $c_1, c_2, c_3, c_4 \in \mathbb{N}$ and some power $q > 1$ of p is contained in $\mathcal{M}(\mathcal{O}, s, t)$. Note that the set in Example 1.6 is a special case in which $c_1 = m_0$, $c_2 = c_3 = 0$, and $c_4 = n_0$. Let $p = 7$, $L = \mathbb{F}_7(x,y)$, $\mathcal{O} = \mathbb{F}_7[x+y, xy]$, $K = \mathrm{Frac}(\mathcal{O})$, $s = x$, $t = 3x + 2y$. For $i, j \in \mathbb{N}$ and $m = n = 7^i + 7^j$, it is not difficult to show directly that $s^m \in \mathcal{O}[t^n]$ and $t^n \in \mathcal{O}[s^m]$; in other words $(m,n) \in \mathcal{M}(\mathcal{O}, s, t)$.

We need the following:

Definition 1.8. *Let $a_1, a_2, a_3, a_4 \in \mathbb{Q}$, define:*

$$F(q; a_1, a_2, a_3, a_4) := \{(a_1 q^i + a_2 q^j, a_3 q^i + a_4 q^j) : i, j \in \mathbb{N}_0\} \subset \mathbb{Q}^2.$$

We will obtain a list of unit equations from the equation $\mathcal{O}[s^m] = \mathcal{O}[t^n]$, then the sets $F(q; a_1, \ldots, a_4)$ in Definition 1.8 correspond to the non-degenerate solutions. Degenerate solutions will correspond to the following sets:

Definition 1.9. *Let s and t be integral over $\mathcal{O}$ and separable over K. Define:*

$$\mathcal{A}_{\mathcal{O},s,t} = \{(m,n) \in \mathbb{N}^2 : \frac{s^m}{t^n} \in \mathcal{O}^*\},$$

$$\mathcal{B}_{\mathcal{O},s,t} = \{(m,n) \in \mathbb{N}^2 : [K(t^n) : K] = 2 \text{ and } \frac{s^m}{\sigma(t^n)} \in \mathcal{O}^*\}$$

where σ in the definition of $\mathcal{B}_{\mathcal{O},q,r}$ is the nontrivial automorphism of the quadratic extension $K(t^n)/K$. Finally, we define:

$$\mathcal{C}_{\mathcal{O},s,t} = \{(m,n) \in \mathbb{N}^2 : \ s^m t^n \in \mathcal{O}^*\}.$$

By the same arguments in [Ngu15, pp. 2–3], we have that each of the sets $\mathcal{A}(\mathcal{O},s,t)$, $\mathcal{B}(\mathcal{O},s,t)$, and $\mathcal{C}(\mathcal{O},s,t)$ is a subset of $\mathcal{M}(\mathcal{O},s,t)$. We can now state the second main result of this paper. As in [Ngu15, pp. 2], for simplicity we *assume the very mild condition that* $\{s^n, t^n : \ n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$. If $s^n \in \mathcal{O}$ or $t^n \in \mathcal{O}$ for some n, Problem (B) becomes much easier and is treated in Section 5 (compare [Ngu15, Section 5]).

Theorem 1.10. *Let s and t be integral over $\mathcal{O}$, separable over K, and satisfy $\{s^n, t^n : \ n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$. Then the set*

$$\mathcal{M}(\mathcal{O},s,t) \setminus (\mathcal{A}(\mathcal{O},s,t) \cup \mathcal{B}(\mathcal{O},s,t) \cup \mathcal{C}(\mathcal{O},s,t))$$

is contained in a finite union of sets of the form

$$F(q; c_1, c_2, c_3, c_4) = \{(c_1 q^i + c_2 q^j, c_3 q^i + c_4 q^j) : \ i,j \in \mathbb{N}_0\}$$

for some power $q > 1$ of p and $c_1, c_2, c_3, c_4 \in \mathbb{Q}$.

Example 1.7 shows that *in general* we cannot improve Theorem 1.10 in the sense that the sets $F(q; c_1, c_2, c_3, c_4)$ appearing in $\mathcal{M}(\mathcal{O},s,t) \setminus \ (\mathcal{A}(\mathcal{O},s,t) \cup \mathcal{B}(\mathcal{O},s,t) \cup \mathcal{C}(\mathcal{O},s,t))$ consist of pairs (m,n) where each of m and n is a linear combination of q^i and q^j for 2 parameters $i,j \in \mathbb{N}$. While we expect the number of sets $F(q; c_1, c_2, c_3, c_4)$ in Theorem 1.10 could be bounded uniformly in terms of $q(K)$, $|S|$ and $[K(s,t) : K]$, our proof does not seem to yield this. The proofs of Theorem 1.2, Corollary 1.4, and Theorem 1.10 are not effective.

The organization of this paper is as follows. In the next section, we introduce finiteness results for unit equations in both zero and positive characteristics. After that, we prove Theorem 1.2, Corollary 1.4, and Theorem 1.10. The last section addresses the easy case of Problem (B) when $\{s^n, t^n : \ n \in \mathbb{N}\} \cap \mathcal{O} \neq \emptyset$.

Acknowledgments. We wish to thank Professors Jan-Hendrik Evertse, Dragos Ghioca, Kálmán Győry, and David Masser for useful discussions. The second author is grateful to Professors Evertse and Győry for answering many questions and sharing the draft of their upcoming book on the topics (in characteristic zero) presented in this paper.

2. Unit Equations

Let $n \in \mathbb{N}$, a solution $(x_1, \ldots, x_n)$ of the equation $a_1 X_1 + \ldots + a_n X_n = 1$ with non-zero parameters a_i's is called *non-degenerate* if no subsums vanish. In other words, there is no proper subset $\emptyset \neq J \subset \{1, \ldots, n\}$ such that $\sum_{j \in J} a_j x_j = 0$.

We start with a celebrated result on unit equation in characteristic zero proved by Evertse, Schlickewei, and Schmidt [ESS02]:

Proposition 2.1. *Let L be a field of characteristic 0 and let G be a finitely generated subgroup of L^* having rank r. Let $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in L^*$, then the number of non-degenerate solutions $(x_1, \ldots, x_n) \in G^n$ of the equation:*

$$a_1 X_1 + \ldots + a_n X_n = 1$$

is at most $\exp\big((6n)^{3n}(nr+1)\big)$.

Now we consider unit equations in positive characteristic where, as usual, subtle issues arise due to the presence of the Frobenius automorphism. For the rest of this section, let L be a field of characteristic p and let G be a subgroup of L^*. The radical of G in L is defined to be:

$$\sqrt[L]{G} := \{\gamma \in L : \ \gamma^m \in G \text{ for some } m \in \mathbb{N}\}.$$

Assume that the group $\sqrt[L]{G}$ is finitely generated. When L is finitely generated over $\mathbb{F}_p$, finite generation of $\sqrt[L]{G}$ is equivalent to that of G. We have the following result by Derksen and Masser:

Proposition 2.2. *Let $a_1, \ldots, a_n \in L^*$. Consider the equation $a_1x_1 + \ldots + a_nx_n = 1$ with $(x_1, \ldots, x_n) \in G^n$. Then there is a finite set $\mathscr{S}$ (contained in $\bar{L}^*$) such that every non-degenerate solution $(x_1, \ldots, x_n)$ has the form:*

$$x_k = \alpha_{k,0}\alpha_{k,1}^{p^{i_1}} \ldots \alpha_{k,n-1}^{p^{i_{n-1}}} \text{ for } k = 1, \ldots, n$$

for some $i_1, \ldots, i_{n-1} \in \mathbb{N}_0$, and $\alpha_{k,j} \in \mathscr{S}$ for $0 \le j \le n-1$.

Proof. This follows from [DM12, Theorem 3] where the form of the x_k's follows from the dehomogenization of points in the set $(\pi_0, \ldots, \pi_h)_p$ (with $h \le n-1$) given in [DM12, Theorem 3]. Earlier versions of this result were obtained by Moosa-Scanlon [MS04] and Ghioca [Ghi08] (see the comments in [DM12, pp. 1050]). □

We use Proposition 2.2 to obtain the following:

Proposition 2.3. *Consider the equation $x_1 + \ldots + x_n = 1$ with $(x_1, \ldots, x_n) \in G^n$. Then there is a positive integer C and a finite set $\mathscr{S}'$ (contained in $\bar{L}^*$) such that for every non-degenerate solution $(x_1, \ldots, x_n)$, we have:*

$$x_k^{p^C} = \alpha_{k,1}^{p^{i_1}} \ldots \alpha_{k,n-1}^{p^{i_{n-1}}} \text{ for } k = 1, \ldots, n$$

for some $i_1, \ldots, i_{n-1} \in \mathbb{N}_0$, and $\alpha_{k,j} \in \mathscr{S}'$ for $1 \le j \le n-1$.

In other words, this says that for every non-degenerate solution of the equation $x_1 + \ldots + x_n = 1$, after raising to some p^C-th power, we can omit the "translation by $(\alpha_{1,0}, \ldots, \alpha_{n,0})$" in the description given in Proposition 2.2. We refer the readers to Question 2.7 for further refinement in this direction. To prove Proposition 2.3, we need the following simple lemma:

Lemma 2.4. *Let $N \ge 1$ and let $e_1, \ldots, e_N$ be integers. There exist C_1 depending on N and the e_i's such that the following holds. For every $u_1, \ldots, u_N \in \mathbb{Z}$ satisfying two conditions:*

(i) $\sum_{i=1}^N e_i p^{u_i} \in \mathbb{Z} \setminus \{0\}$,
(ii) *there does not exist a non-empty proper subset $J \subset \{1, \ldots, N\}$ such that $\sum_{i \in J} e_i p^{u_i} = 0$,*

we have that $u_i + C_1 \ge 0$ for every $1 \le i \le N$.

Proof. Induction on N, the case $N = 1$ gives that $u_1 + \mathrm{ord}_p(e_1) \ge 0$. Now let $N \ge 2$ and assume that the lemma holds for every smaller value of N. Since $|\sum_{i=1}^N e_i p^{u_i}| \ge 1$, there is a lower bound $-C_2$ on $\max\{u_1, \ldots, u_N\}$. Say $u_N = \max\{u_i\}_i$, then apply the induction hypothesis for $e_1 p^{u_1 + C_2} + \ldots + e_{n-1} p^{u_{N-1} + C_2}$. □

Remark 2.5. When some e_i in Lemma 2.4 is zero, the lemma is vacuously true for any choice C_1 since there do not exist $u_1, \ldots, u_N$ satisfying the conditions (i) and (ii). If this is the case, we will simply choose $C_1 = 0$.

Proof of Proposition 2.3. Let $\mathscr{S}$ be a finite set satisfying the conclusion of Proposition 2.2 for the unit equation $x_1 + \ldots + x_n = 1$. Let Γ be the group generated by $\mathscr{S}$ and let r denote its rank. For every $x \in \Gamma$, let $\bar{x}$ denote its image in $\Gamma/\Gamma_{\mathrm{tors}}$. Let $g_1, \ldots, g_r \in \Gamma$ such that $\{\bar{g}_i : \ 1 \le i \le r\}$ is a basis of $\Gamma/\Gamma_{\mathrm{tors}}$. Let $E_1, \ldots, E_r$ be the functions from Γ to $\mathbb{Z}$ satisfying:

$$\bar{x} = \prod_{\ell=1}^{r} \bar{g}_\ell^{E_\ell(x)}$$

for every $x \in \Gamma$. Define:

$$\tilde{\mathscr{S}} := \left\{ \prod_{\ell=1}^{r} g_\ell^{d_\ell} : \ d_\ell \in \{0\} \cup E_\ell(\mathscr{S}) \text{ for } 1 \le \ell \le r \right\}. \tag{1}$$

Then the desired set $\mathscr{S}'$ is defined as follows:

$$\mathscr{S}' := \{\alpha\beta : \ \alpha \in \Gamma_{\mathrm{tors}}, \ \beta \in \tilde{\mathscr{S}}\}. \tag{2}$$

Let $(x_1, \ldots, x_n)$ be a non-degenerate solution of the given unit equation. For every $m \in \mathbb{N}_0$, $(x_1^{p^m}, \ldots, x_n^{p^m})$ is also a non-degenerate solution. By the definition of $\mathscr{S}$, we have:

$$x_k^{p^m} = \alpha_{k,0,m} \alpha_{k,1,m}^{p^{i_{1,m}}} \ldots \alpha_{k,n-1,m}^{p^{i_{n-1,m}}} \text{ for } k = 1, \ldots, n \text{ and for } m \in \mathbb{N}_0 \tag{3}$$

for some $i_{1,m}, \ldots, i_{n-1,m} \in \mathbb{N}_0$, and $\alpha_{k,j,m} \in \mathscr{S}$ for $0 \le j \le n-1$. Since $\mathscr{S}$ is finite, we may assume that (3) holds for infinitely many m for *one* tuple $(\alpha_{k,j})$. In other words, there is an infinite subset $\mathcal{M}_1$ of $\mathbb{N}_0$ such that:

$$x_k^{p^m} = \alpha_{k,0} \alpha_{k,1}^{p^{i_{1,m}}} \ldots \alpha_{k,n-1}^{p^{i_{n-1,m}}} \text{ for } k = 1, \ldots, n \text{ and for } m \in \mathcal{M}_1 \tag{4}$$

for some $i_{1,m}, \ldots, i_{n-1,m} \in \mathbb{N}_0$, and $\alpha_{k,j} \in \mathscr{S}$ for $0 \le j \le n-1$. Write:

$$\bar{x}_k = \prod_{\ell=1}^{r} \bar{g}_\ell^{b_{k,\ell}} \text{ for } 1 \le k \le n. \tag{5}$$

$$\bar{\alpha}_{k,j} = \prod_{\ell=1}^{r} g_\ell^{e_{k,j,\ell}} \text{ for } 1 \le k \le n \text{ and } 0 \le j \le n-1. \tag{6}$$

Therefore $p^m b_{k,\ell} = e_{k,0,\ell} + e_{k,1,\ell} p^{i_{1,m}} + \ldots + e_{k,n-1,\ell} p^{i_{n-1,m}}$ for $1 \le k \le n$ and $m \in \mathcal{M}_1$.

For each $1 \le k \le n$ and $1 \le \ell \le r$, we claim that for all but finitely many $m \in \mathcal{M}_1$, $p^m b_{k,\ell}$ is a (not necessarily proper) subsum of $e_{k,1,\ell} p^{i_{1,m}} + \ldots + e_{k,n-1,\ell} p^{i_{n-1,m}}$. Indeed, there is nothing to prove when $e_{0,\ell} = 0$; when $e_{0,\ell} \neq 0$, this follows from Proposition 2.1. We now exclude those finitely many m's from $\mathcal{M}_1$ as in the claim and let $\mathcal{M}_2$ denote the resulting infinite set.

Let Λ be the set of pairs (k, ℓ) with $1 \le k \le n$ and $1 \le \ell \le r$ such that $b_{k,\ell} \neq 0$. For every $(k, \ell) \in \Lambda$ and for every (non-empty) subset J of $\{1, \ldots, n-1\}$ consider the set $M(k, \ell, J) \subseteq \mathcal{M}_2$ of m satisfying the following conditions:

(i) $p^m b_{k,\ell} = \sum_{j \in J} e_{k,j,\ell} p^{i_{j,m}}$.

(ii) The sum $\sum_{j \in J} e_{k,j,\ell} p^{i_{j,m}}$ has no vanishing proper subsum.

By the above claim, we have: $\bigcup_J M(k,\ell,J) = \mathcal{M}_2$ where J ranges over all the non-empty subsets of $\{1,\dots,n-1\}$. Obviously, this gives:

$$\bigcap_{(k,\ell)\in\Lambda}\left(\bigcup_J M(k,\ell,J)\right) = \mathcal{M}_2.$$

Therefore it is possible to choose a non-empty subset $\mathscr{J}_{k,\ell}$ of $\{1,\dots,n-1\}$ for each $(k,\ell)\in\Lambda$ such that the set

$$\mathcal{M}_3 := \bigcap_{(k,\ell)\in\Lambda} M(k,\ell,\mathscr{J}_{k,\ell})$$

is infinite.

Pick one $m'\in\mathcal{M}_3$. By the definition of $\mathcal{M}_3$ and the sets $M(k,\ell,\mathscr{J}_{k,\ell})$, we have the following:

(i) $b_{k,\ell} = \sum_{j\in\mathscr{J}_{k,\ell}} e_{k,j,\ell}p^{i_{j,m'}-m'}$ for every $(k,\ell)\in\Lambda$.

(ii) The sum $\sum_{j\in\mathscr{J}_{k,\ell}} e_{k,j,\ell}p^{i_{j,m'}-m'}$ has no vanishing proper subsum for every $(k,\ell)\in\Lambda$.

Now we let Ω range over all non-empty subset of $\{1,\dots,n\}\times\{1,\dots,r\}$, let $(J_{k,\ell})_{(k,\ell)\in\Omega}$ range over all possible $|\Omega|$-tuple of non-empty subsets of $\{1,\dots,n-1\}$, and let C be the maximum of all the C_1's obtained when applying Lemma 2.4 for the tuples $(e_{k,j,\ell})_{j\in J_{k,\ell}}$ for $(k,\ell)\in\Omega$ (see Remark 2.5).

We have:

$$p^C b_{k,\ell} = \sum_{j\in\mathscr{J}_{k,\ell}} e_{k,j,\ell}p^{i_{j,m'}-m'+C} = \sum_{j=1}^{n-1} f_{k,j,\ell}p^{i_{j,m'}-m'+C} \tag{7}$$

for every $1\le\ell\le r$ where $f_{k,j,\ell} := e_{k,j,\ell}$ if $(k,\ell)\in\Lambda$ and $j\in\mathscr{J}_{k,\ell}$; otherwise $f_{k,j,\ell} := 0$. This implies that $f_{k,j,\ell}\in\{0\}\cup E_\ell(\mathscr{S})$ for every $1\le k\le n$, $1\le j\le n-1$, and $1\le\ell\le r$. Hence the element:

$$\beta_{k,j} := \prod_{\ell=1}^{r} g_\ell^{f_{k,j,\ell}} \text{ belongs to } \tilde{\mathscr{S}} \text{ for } 1\le k\le n \text{ and } 1\le j\le n-1.$$

Let $i'_j = i_{j,m'} - m' + C$ which is non-negative for $1\le j\le n-1$ by the definition of C. By (5), (7), and the definition of the $\beta_{k,j}$'s, we have:

$$x_k^{p^C} \equiv \beta_{k,1}^{p^{i'_1}}\dots\beta_{k,n-1}^{p^{i'_{n-1}}} \text{ in } \Gamma/\Gamma_{\mathrm{tors}}$$

for $1\le k\le n$. Since Γ_{tors} is a finite cyclic group whose order is relatively prime to p, for $1\le k\le n$ there is $\zeta_k\in\Gamma_{\mathrm{tors}}$ such that:

$$x_k^{p^C} = (\zeta_k\beta_{k,1})^{p^{i'_1}}\beta_{k,2}^{p^{i'_2}}\dots\beta_{k,n-1}^{p^{i'_{n-1}}}.$$

This shows that the pair $(C,\mathscr{S}')$ satisfies the desired conclusion. □

When $n=2$, we have a more precise result:

Proposition 2.6. *Let r denote the rank of G and consider the equation $x+y=1$ with $(x,y)\in G^2$. We have:*

(a) *There exists a finite subset* $\mathscr{X}$ *of* $L^* \times L^*$ *of size at most* $p^{2r}-1$ *such that every solution* $(x,y) \in G^2 \setminus \bar{\mathbb{F}}_p^2$ *has the form* $x = x_0^{p^k}$ *and* $y = y_0^{p^k}$ *for some* $(x_0, y_0) \in \mathscr{X}$ *and* $k \in \mathbb{N}_0$.

(b) *There exists a finite subset* $\mathscr{X}'$ *of* $L^* \times L^*$ *of size at most* p^{2r} *such that every solution* $(x,y) \in G^2$ *has the form* $x = x_0^{p^k}$ *and* $y = y_0^{p^k}$ *for some* $(x_0, y_0) \in \mathscr{X}'$ *and* $k \in \mathbb{N}_0$.

Proof. We prove (a) first. Write $H = \sqrt[L]{G}$ which is finitely generated by our assumption. Note that H/G is a torsion abelian group and so the rank of H is r. We first consider solutions to the equation $x+y=1$ with $(x,y) \in H \times H$. We have that $H \cong \mathbb{Z}^r \times \mathbb{F}_q^*$ where $\mathbb{F}_q = L \cap \bar{\mathbb{F}}_p$. Since the Frobenius map is surjective on $\mathbb{F}_q^*$ we have that $H/H^p \cong (\mathbb{Z}/p\mathbb{Z})^r$. Let $1 = \epsilon_0, \ldots, \epsilon_{p^r-1}$ be a set of coset representatives for H/H^p. Let $(i,j) \in \{0,1,\ldots,p^r-1\}^2$ with $(i,j) \neq (0,0)$. We now consider all solutions to the equation $x+y=1$ with $(x,y) \in H^p\epsilon_i \times H^p\epsilon_j$. Observe that at least one of ϵ_i, ϵ_j cannot be in $L^{\langle p \rangle} := \{a^p \colon a \in L\}$. Otherwise, we would have $\epsilon_i = a^p$ and $\epsilon_j = b^p$ for some $a, b \in L$. Since $H = \sqrt[L]{G}$ we would then have $a, b \in H$ and so $\epsilon_i, \epsilon_j \in H^p$ contradicting our choice that $(i,j) \neq (0,0)$.

We assume that $\epsilon_i \notin L^{\langle p \rangle}$, the case when $\epsilon_j \notin L^{\langle p \rangle}$ can be handled similarly. Then the sum $L^{\langle p \rangle} + L^{\langle p \rangle}\epsilon_i$ is direct. On the other hand, if $L^{\langle p \rangle} + L^{\langle p \rangle}\epsilon_i + L^{\langle p \rangle}\epsilon_j$ is direct then there cannot be any solutions to the equation $x+y=1$ with $(x,y) \in H^p\epsilon_i \times H^p\epsilon_j$. Thus it suffices to consider the case when $\epsilon_j = a^p + b^p\epsilon_i$ with $a, b \in L$. Note that the pair (a,b), if exists, is unique. Write $x = x_1^p\epsilon_i$ and $y = y_1^p\epsilon_j$, then the equation $x+y=1$ gives:

$$x_1^p\epsilon_i + y_1^p\epsilon_j = (ay_1)^p + (x_1^p + b^p y_1^p)\epsilon_i = 1.$$

This gives $ay_1 = 1$ and $x_1 + by_1 = 0$ since $L^{\langle p \rangle} + L^{\langle p \rangle}\epsilon_i$ is direct. Therefore (x_1, y_1) and, hence, (x,y) are uniquely determined. Overall, we have at most $p^{2r}-1$ solutions to the equation $x+y=1$ with $(x,y) \in H \times H$ and $(x,y) \notin H^p \times H^p$. Let $M \leq p^{2r}-1$ and let $(x_i, y_i) \in H \times H$ with $i = 1, \ldots, M$ denote the collection of all such solutions. Then if $(x,y) \in H \times H$ is a solution to $x+y=1$ with x and y not algebraic over $\mathbb{F}_p$ then there is some largest m such that $(x,y) \in H^{p^m} \times H^{p^m}$. Therefore there must exist some $i \in \{1, \ldots, M\}$ such that $x = x_i^{p^m}$ and $y = y_i^{p^m}$.

We now consider the solutions (x,y) in $G \times G$. For each $i \in \{1, \ldots, M\}$, consider the set N_i of all nonnegative integers n for which $x_i^{p^n}$ and $y_i^{p^n}$ are both in G. This set is either empty or has some least element n_i. Letting I denote the set of $i \in \{1, \ldots, M\}$ for which N_i is nonempty and then letting $\mathscr{X} = \{(x_i^{p^{n_i}}, y_i^{p^{n_i}}) \colon i \in I\}$ we obtain the desired conclusion for solutions to $x+y=1$ with $(x,y) \in G \times G$.

For part (b), we fix a generator γ of $\mathbb{F}_q^*$. Then every solution $(x,y) \in (\mathbb{F}_q^*)^2$ of $x+y=1$ has the form $(x = \gamma^{p^k}, y = (1-\gamma)^{p^k})$ for some $k \in \mathbb{N}_0$. Let n be the smallest integer in $\mathbb{N}_0$ such that $(\gamma^{p^n}, (1-\gamma)^{p^n}) \in G^2$ *if there exists such an* n, then define

$$\mathscr{X}' := \mathscr{X} \cup \{(\gamma^{p^n}, (1-\gamma)^{p^n})\}.$$

Otherwise, if such an n does not exist, define $\mathscr{X}' := \mathscr{X}$. □

In view of Proposition 2.3 and Proposition 2.6, we ask the following question:

Question 2.7. *Consider the equation* $x_1 + \ldots + x_n = 1$ *with* $x_1, \ldots, x_n \in G$. *Is it true that there is a finite set* $\mathscr{S}' \subset L^*$ *whose size is bounded only in terms of* n,

the rank, and torsion of $\sqrt[L]{G}$ *such that every non-degenerate solution* $(x_1, \dots, x_n)$ *has the form:*

$$x_k = \alpha_{k,1}^{p^{i_1}} \dots \alpha_{k,n-1}^{p^{i_{n-1}}} \text{ for } k = 1, \dots, n$$

for some $i_1, \dots, i_{n-1} \in \mathbb{N}_0$, *and* $\alpha_{k,j} \in \mathscr{S}'$ *for* $0 \le j \le n-1$.

3. Proof of Theorem 1.2 and Corollary 1.4

3.1. **Notation and some preliminary results.** For every finite separable extension E/K, let $\mathcal{O}_E$ denote the integral closure of $\mathcal{O}$ in E, and let $q(E)$ be the cardinality of the finite field $\bar{\mathbb{F}}_p \cap E$. Let M_E denote the discrete valuations on E extending those in M_K and normalized such that the value group of E^* is $\mathbb{Z}$. Let S_E denote the finite subset of S lying above S. We have the following:

Lemma 3.1. *Let* E *be a finite separable extension of* K *and let* T *be a finite subset of* M_E *containing* S_E. *Then* $q(E) \le q(K)^{[E:K]}$ *and the rank of* $\mathcal{O}_{E,T}^*$ *is at most* $|T| - 1$. *Consequently, the rank of* $\mathcal{O}_E^*$ *is at most* $[E : K]|S| - 1$.

Proof. For every $\zeta \in \bar{\mathbb{F}}_p \cap E$, we have that $[K(\zeta) : K]$ divides $[E : K]$. Since the minimal polynomial of ζ over K must have coefficients in $\mathbb{F}_{q(K)} = \bar{\mathbb{F}}_p \cap K$, we have that $[K(\zeta) : K] = [\mathbb{F}_{q(K)}(\zeta) : \mathbb{F}_{q(K)}]$. Hence ζ is contained in the finite field of degree $[E : K]$ over $\mathbb{F}_{q(K)}$. This proves the first assertion.

Let $\mathrm{Div}(T)$ denote the free abelian group generated by T. Consider the homomorphism $\mathcal{O}_{E,T}^* \to \mathrm{Div}(T)$ defined by $a \mapsto \sum_{v \in T} n_v v(a) v$. Since its kernel is exactly $(\mathcal{O}_{K,T}^*)_{\mathrm{tors}}$ and its image is contained in the subgroup consisting of elements whose sum of coefficients is zero, we have that the rank of $\mathcal{O}_{E,T}^*$ is at most $|T| - 1$.

Consequently, the rank of $\mathcal{O}_E^*$ is at most $|S_E| - 1$. Since $|S_E| \le [E : K]|S|$ (see [Neu99, pp. 164]), we get the desired conclusion. □

We will need the following result on unit equations in characteristic zero:

Lemma 3.2. *Let* A *and* B *be distinct non-zero integers neither of which is divisible by* p. *Consider the equation:*

$$Ap^{X_1} - Ap^{X_2} + Bp^{X_3} - Bp^{X_4} = 0 \text{ for } X_1, \dots, X_4 \in \mathbb{N}_0 \tag{8}$$

Then there exists a set $\mathscr{D}$ *(depending on* p, A, *and* B*) of size at most* $\exp(4 \times 18^9) + 1$ *such that every solution* (x_1, x_2, x_3, x_4) *of* (8) *satisfies* $(x_3 - x_4) - (x_1 - x_2) \in \mathscr{D}$.

Proof. Dividing by Bp^{X_4}, we have:

$$\frac{A}{B} p^{X_1 - X_4} - \frac{A}{B} p^{X_2 - X_4} + p^{X_3 - X_4} = 1 \tag{9}$$

with the solution $\mathbf{u} = (x_1 - x_4, x_2 - x_4, x_3 - x_4)$. There are four cases:

(a) No proper subsums of the left hand side of (9) vanish. Proposition 2.1 shows that there are at most $\exp(4 \times 18^9)$ possibilities for $\mathbf{u}$. Hence at most $\exp(4 \times 18^9)$ possibilities for $(x_3 - x_4) - (x_1 - x_4) + (x_2 - x_4) = (x_3 - x_4) - (x_1 - x_2)$.

(b) $p^{x_3 - x_4} = 1$ and $p^{x_1 - x_4} - p^{x_2 - x_4} = 0$. This implies $(x_3 - x_4) - (x_1 - x_2) = 0$.

(c) $-\frac{A}{B} p^{x_2 - x_4} = 1$ and $\frac{A}{B} p^{x_1 - x_4} + p^{x_3 - x_4} = 0$. Since $\gcd(A, p) = \gcd(B, p) = 1$, we must have that $A = -B$, $x_2 = x_4$ and $x_1 = x_3$. This gives $(x_3 - x_4) - (x_1 - x_2) = 0$.

(d) $\frac{A}{B}p^{x_1-x_4}=1$ and $-\frac{A}{B}p^{x_2-x_4}+p^{x_3-x_4}=0$. Since $\gcd(A,p)=\gcd(B,p)=1$, we must have that $A=B$. Since we assume that $A\neq B$, this case cannot happen.

The desired set $\mathscr{D}$ is obtained from the possibilities of $(x_3-x_4)-(x_1-x_2)$ in Case (a) together with the element 0 from Cases (b) and (c). □

3.2. **Proof of Theorem 1.2.** Throughout this subsection, assume the notation in Theorem 1.2 and let L denote the Galois closure of $K(s)$ in $\overline{K}$. The case $d:=[K(s):K]=2$ is immediate, as follows. Assume $\mathcal{O}[s]=\mathcal{O}[t]$, then we can write $t=\alpha s+\beta$ and $s=\gamma t+\delta$ for unique $\alpha,\beta,\gamma,\delta\in\mathcal{O}$. This implies that $\alpha\gamma=1$, hence $\alpha\in\mathcal{O}^*$. This proves Theorem 1.2 when $d=2$ (with $t_1=s$). For the rest of the proof, we assume $d\geq 3$.

Write $q(L)=p^\lambda$. By Lemma 3.1, we have:

$$q(L)\leq q(K)^{[L:K]}\leq q(K)^{d!},\ \text{hence}\ \lambda\leq d!\log_p(q(K)). \tag{10}$$

Let $\{\mathrm{id}=\sigma_1,\dots,\sigma_d\}$ be a choice of representatives of the left cosets of $\mathrm{Gal}(L/K(s))$ in $\mathrm{Gal}(L/K)$. For every element $\alpha\in K(s)$ and for $1\leq i\leq d$, we denote $\alpha_{(i)}=\sigma_i(\alpha)$. In particular, $s=s_{(1)},\dots,s_{(d)}$ are all the conjugates of s over K. Let G be the radical in L of the group generated by the following:

(i) The group of units of $\mathcal{O}[s_{(i)}-s_{(j)}]$ for $1\leq i\neq j\leq d$.
(ii) The elements $s_{(i)}-s_{(j)}$ for $1\leq i\neq j\leq d$.

Let r denote the rank of G. By Lemma 3.1 and (10), we have the following:

$$|G_{\mathrm{tors}}|\leq q(L)-1<q(K)^{d!}\ \text{and}\ r\leq\frac{d(d-1)}{2}(d^2|S|-1)+\frac{d(d-1)}{2}<d^4|S|. \tag{11}$$

The rest of this subsection is used to prove the following more precise version of Theorem 1.2:

Theorem 3.3. *There are* $N\leq\left(\min\{q(L),q(K)^{d^3}\}\right)^{d^3}+\left(\exp(18^{10})p^{2r}d^8\lambda\right)^{d^3}$ *elements* $t_1,\dots,t_N$ *satisfying the conditions (a) and (b) of Theorem 1.2.*

Remark 3.4. By (10), (11), and Theorem 3.3, the bound in Theorem 3.3 is less than $q(K)^{d^6}+(\exp(18^{10})p^{2d^4|S|}d^8(d!)\log_p(q(K)))^{d^3}$ which is less than

$$q(K)^{d^6}+\left(\exp(18^{10})p^{3d^4|S|}\log_p q(K)\right)^{d^3}.$$

This proves Theorem 1.2. Note that if we simply used $q(L)$ instead of $\min\{q(L),q(K)^{d^3}\}$ for the bound in Theorem 3.3, then we would, a priori, have the *doubly exponential* expression $q(K)^{d!d^3}$ instead of $q(K)^{d^6}$ for the bound in Theorem 1.2.

Now assume that t satisfies $\mathcal{O}[t]=\mathcal{O}[s]$. By writing $t=P_1(s)$ and $s=P_2(t)$ for polynomials $P_1(X),P_2(X)\in\mathcal{O}[X]$, we have that for $1\leq i\neq j\leq d$:

$$\frac{t_{(i)}-t_{(j)}}{s_{(i)}-s_{(j)}}\in(\mathcal{O}[s_{(i)},s_{(j)}])^*,\ \text{hence}\ t_{(i)}-t_{(j)}\in G. \tag{12}$$

This implies that for every triple (i,j,k) of distinct elements in $\{1,\dots,d\}$, the elements:

$$x=(t_{(i)}-t_{(j)})/(t_{(k)}-t_{(j)})$$
$$y=(t_{(k)}-t_{(i)})/(t_{(k)}-t_{(j)})$$

give a solution to $X+Y=1$ with $x,y\in G$.

By Proposition 2.6, there exists a subset $\{(x_i, y_i) : 1 \leq i \leq M\}$ of L^* of size $M \leq p^{2r}$ such that each solution (x, y) to $X + Y = 1$ with $x, y \in G$ is of the form $(x_i^{p^j}, y_i^{p^j})$ for some $i \in \{1, \dots, M\}$ and $j \in \mathbb{N}_0$. Moreover, we may assume that $x_i \notin L^{\langle p \rangle}$ whenever $x_i \notin \bar{\mathbb{F}}_p$.

Let $\mathscr{T}(d)$ denote the set of all triples (i, j, k) of distinct $i, j, k \in \{1, \dots, d\}$ (hence $|\mathscr{T}(d)| = d(d-1)(d-2)$). Now for each sequence $\mathbf{m} := (m_{i,j,k}) \in \{1, \dots, M\}^{\mathscr{T}(d)}$ indexed by the triples $(i, j, k) \in \mathscr{T}(d)$, consider the set $X_{\mathbf{m}}$ of all $t \in \mathcal{O}[s]$ for which $\mathcal{O}[t] = \mathcal{O}[s]$ and such that there exists some sequence of non-negative integers $\mathbf{a} := (a_{i,j,k})$ (indexed by $(i, j, k) \in \mathscr{T}(d)$) satisfying:

$$(t_{(i)} - t_{(j)})/(t_{(k)} - t_{(j)}) = x_{m_{i,j,k}}^{p^{a_{i,j,k}}} \tag{13}$$

for all $(i, j, k) \in \mathscr{T}(d)$. We let $T_{\mathbf{m}}$ denote the set of triples $(i, j, k) \in \mathscr{T}(d)$ such that $x_{m_{i,j,k}} \notin \bar{\mathbb{F}}_p$. If $t \in X_{\mathbf{m}}$ and $(i, j, k) \in T_{\mathbf{m}}$ then $a_{i,j,k}$ is determined uniquely from (13).

The case when $T_{\mathbf{m}} = \emptyset$ (i.e. $x_{m_{i,j,k}} \in \bar{\mathbb{F}}_p^*$ for every (i, j, k)) is rather easy, as follows:

Lemma 3.5. *Let* $X_{\mathrm{alg}} := \bigcup_{\mathbf{m}:\ T_{\mathbf{m}} = \emptyset} X_{\mathbf{m}}$. *There are at most* $\left(\min\{q(L), q(K)^{d^3}\}\right)^{d^3}$ *elements* $t_1, \dots, t_N \in X_{\mathrm{alg}}$ *such that every* $t \in X_{\mathrm{alg}}$ *has the form* $t = at_i + b$ *for some* $1 \leq i \leq N$, $a \in \mathcal{O}^*$, *and* $b \in \mathcal{O}$.

Proof. Define the relation $\approx$ in X_{alg} as follows. Let $t, t' \in X_{\mathrm{alg}}$, define $t \approx t'$ if $t' = at + b$ for some $a \in \mathcal{O}^*$ and $b \in \mathcal{O}$. It is immediate that this is an equivalence relation. It remains to show that in every subset $\mathscr{A}$ of X_{alg} having more than $\left(\min\{q(L), q(K)^{d^3}\}\right)^{d^3}$ elements, there exist two elements that are equivalent to each other.

For $(i, j, k) \in \mathscr{T}(d)$, let $\mu_{i,j,k} = \bar{\mathbb{F}}_p^* \cap K(s_{(i)}, s_{(j)}, s_{(k)}) \subseteq \mathbb{F}_{q(L)}^*$. Hence $|\mu_{i,j,k}| \leq \min\{q(L), q(K)^{d^3}\}$ by Lemma 3.1. For $t \in X_{\mathrm{alg}}$, we have $\dfrac{t_{(i)} - t_{(j)}}{t_{(k)} - t_{(j)}} \in \mu_{i,j,k}$ for every $(i, j, k) \in \mathscr{T}(d)$. Since $|\mathscr{A}| > |\prod_{(i,j,k)} \mu_{i,j,k}|$, there exist $t, t' \in \mathscr{A}$ such that $\dfrac{t_{(i)} - t_{(j)}}{t_{(k)} - t_{(j)}} = \dfrac{t'_{(i)} - t'_{(j)}}{t'_{(k)} - t'_{(j)}}$ for every $(i, j, k) \in \mathscr{T}(d)$. Equivalently, the element $a := \dfrac{t'_{(i)} - t'_{(j)}}{t_{(i)} - t_{(j)}}$ is independent of distinct $i, j \in \{1, \dots, d\}$, and belongs to $\mathcal{O}[s_{(i)}, s_{(j)}]^*$ by (12). Hence $a \in \mathcal{O}^*$ since it is non-zero, invariant under $\mathrm{Gal}(L/K)$, and integral over $\mathcal{O}$.

Now the element $b := t'_{(i)} - at_{(i)}$ is independent of $i \in \{1, \dots, d\}$. Hence $b \in \mathcal{O}$ since it is invariant under $\mathrm{Gal}(L/K)$ and integral over $\mathcal{O}$. This finishes the proof. □

It remains to investigate the case $T_{\mathbf{m}} \neq \emptyset$. We have the following useful observation:

Lemma 3.6. *Let* $t' \in X_{\mathbf{m}}$ *and write:*

$$(t'_{(i)} - t'_{(j)})/(t'_{(k)} - t'_{(j)}) = x_{m_{i,j,k}}^{p^{b_{i,j,k}}}$$

for a sequence of non-negative integers $(b_{i,j,k})$. *We have:*

(a) *If* $(i,j,k) \in T_{\mathbf{m}}$ *then* $x_{m_{i,j,k}} = x_{m_{k,j,i}}^{-1}$ *and* $b_{m_{i,j,k}} = b_{m_{k,j,i}}$.
(b) *Let* $\sigma \in \mathrm{Gal}(L/K)$ *and* $(i,j,k) \in T_{\mathbf{m}}$. *Let* $(i_1,j_1,k_1) \in \mathscr{T}(d)$ *be such that* $\sigma(t_{(i)}) = t_{(i_1)}$, $\sigma(t_{(j)}) = t_{(j_1)}$, $\sigma(t_{(k)}) = t_{(k_1)}$. *Then* $\sigma(x_{m_{i,j,k}}) = x_{m_{i_1,j_1,k_1}}$ *and* $b_{i,j,k} = b_{i_1,j_1,k_1}$.

Proof. For part (a), note the identity:

$$x_{m_{i,j,k}}^{p^{b_{i,j,k}}} = \left(x_{m_{k,j,i}}^{p^{b_{k,j,i}}}\right)^{-1}.$$

This implies that $x_{m_{k,j,i}}$ is not in $\bar{\mathbb{F}}_p$ either; hence both $x_{m_{i,j,k}}$ and $x_{m_{j,k,i}}$ are not in $L^{\langle p\rangle}$ by our choice of the set $\{x_i : 1 \le i \le M\}$. If $b_{i,j,k} < b_{k,j,i}$ (respectively $b_{i,j,k} > b_{k,j,i}$) then we would have $x_{m_{i,j,k}} \in L^{\langle p\rangle}$ (respectively $x_{m_{k,j,i}} \in L^{\langle p\rangle}$), contradiction. Therefore $b_{i,j,k} = b_{k,j,i}$ and $x_{m_{i,j,k}} = x_{m_{k,j,i}}^{-1}$.

For part (b), we argue similarly by using the identity:

$$\sigma(x_{m_{i,j,k}})^{p^{b_{i,j,k}}} = x_{m_{i_1,j_1,k_1}}^{p^{b_{i_1,j_1,k_1}}}.$$

□

We need the following technical result:

Proposition 3.7. *Let* $\mathbf{m} := (m_{i,j,k}) \in \{1,\dots,M\}^{\mathscr{T}(d)}$ *and* $t \in X_{\mathbf{m}}$ *with*

$$(t_{(i)} - t_{(j)})/(t_{(k)} - t_{(j)}) = x_{m_{i,j,k}}^{p^{a_{i,j,k}}}$$

for every $(i,j,k) \in \mathscr{T}(d)$ *for some sequence of non-negative integers* $\mathbf{a} = (a_{i,j,k})$. *There exists a set* $J \subseteq \mathbb{Z}$ *(possibly depending on* $\mathbf{m}$, t, *and* $\mathbf{a}$*) such that the following holds:*

(a) $|J| \le d^4(1 + \exp(4 \times 18^9))$
(b) *For every* $t' \in X_{\mathbf{m}}$, *for* $(i,j,k) \in T_{\mathbf{m}}$, *let* $b_{m_{i,j,k}}$ *be the unique non-negative integer such that*

$$(t'_{(i)} - t'_{(j)})/(t'_{(k)} - t'_{(j)}) = x_{m_{i,j,k}}^{p^{b_{i,j,k}}}.$$

For any four distinct elements $i,j,k,\ell \in \{1,\dots,M\}$ *such that* $(i,j,k) \in T_{\mathbf{m}}$ *and* $(i,j,\ell) \in T_{\mathbf{m}}$, *we have* $(b_{i,j,k} - a_{i,j,k}) - (b_{i,j,\ell} - a_{i,j,\ell})$ *is in* J.

Proof. Since there are less than d^4 quadruples of distinct elements (i,j,k,ℓ), it suffices to fix any four distinct elements i,j,k,ℓ such that (i,j,k) and (i,j,ℓ) are in $T_{\mathbf{m}}$ and prove that there are at most $\exp(4 \times 18^9) + 1$ possibilities (independent of t') for $\Delta := (b_{i,j,k} - a_{i,j,k}) - (b_{i,j,\ell} - a_{i,j,\ell})$. Part (a) of Lemma 3.6 gives $x_{m_{i,j,k}} = x_{m_{k,j,i}}^{-1}$, $x_{m_{i,j,\ell}} = x_{m_{\ell,j,i}}^{-1}$, $a_{m_{i,j,k}} = a_{m_{k,j,i}}$, $b_{m_{i,j,k}} = b_{m_{k,j,i}}$, $a_{m_{i,j,\ell}} = a_{m_{\ell,j,i}}$, and $b_{m_{i,j,\ell}} = b_{m_{\ell,j,i}}$. These identities will be used many times in the proof.

Observe that

$$1 = \frac{(t_{(i)} - t_{(j)})}{(t_{(k)} - t_{(j)})} \cdot \frac{(t_{(k)} - t_{(j)})}{(t_{(\ell)} - t_{(j)})} \cdot \frac{(t_{(\ell)} - t_{(j)})}{(t_{(i)} - t_{(j)})}.$$

This relation gives that

$$1 = x_{m_{i,j,k}}^{p^{a_{i,j,k}}} x_{m_{k,j,\ell}}^{p^{a_{k,j,\ell}}} x_{m_{\ell,j,i}}^{p^{a_{\ell,j,i}}}. \tag{14}$$

Using the similar expression involving $t'_{(i)}, t'_{(j)}, t'_{(k)}, t'_{(\ell)}$ gives

$$1 = x_{m_{i,j,k}}^{p^{b_{i,j,k}}} x_{m_{k,j,\ell}}^{p^{b_{k,j,\ell}}} x_{m_{\ell,j,i}}^{p^{b_{\ell,j,i}}}. \tag{15}$$

Raising both sides of (14) to the power $p^{b_{k,j,\ell}}$ and raising both sides of (15) to the power $p^{a_{k,j,\ell}}$ and then dividing yields

$$1 = x_{m_{i,j,k}}^{p^{a_{i,j,k}+b_{k,j,\ell}}-p^{b_{i,j,k}+a_{k,j,\ell}}} x_{m_{\ell,j,i}}^{p^{a_{\ell,j,i}+b_{k,j,\ell}}-p^{b_{\ell,j,i}+a_{k,j,\ell}}}. \tag{16}$$

We now consider two cases:

Case 1: $x_{m_{i,j,k}}$ and $x_{m_{\ell,j,i}}$ generate a rank two abelian subgroup of L^*. We claim that $b_{i,j,k} - a_{i,j,k} = b_{i,j,\ell} - a_{i,j,\ell}$.

By the assumption in this case and (16), we must have

$$a_{i,j,k} + b_{k,j,\ell} = b_{i,j,k} + a_{k,j,\ell} \text{ and } a_{\ell,j,i} + b_{k,j,\ell} = b_{\ell,j,i} + a_{k,j,\ell}.$$

This implies:

$$b_{i,j,k} - a_{i,j,k} = b_{k,j,\ell} - a_{k,j,\ell} = b_{\ell,j,i} - a_{\ell,j,i}$$

which proves the desired claim. We now simply choose $J(i,j,k,\ell) = \{0\}$ in this case.

Case 2: $x_{m_{i,j,k}}$ and $x_{m_{\ell,j,i}}$ generate a rank one abelian subgroup of L^*. Let Γ be the radical in L of this rank one subgroup and let $u \in L^*$ be a generator of the infinite cyclic group $\Gamma/\Gamma_{\text{tors}}$. Hence $u \notin \bar{\mathbb{F}}_p$ and there exist non-zero integers A and B such that $x_{m_{i,j,k}}u^{-A}$ and $x_{m_{\ell,j,i}}u^{-B}$ are both in $\bar{\mathbb{F}}_p^*$. Due to our choice that $x_{m_{i,j,k}} \notin L^{\langle p\rangle}$ and $x_{m_{\ell,j,i}} \notin L^{\langle p\rangle}$, neither A nor B is divisible by p. Now (16) gives:

$$A(p^{a_{i,j,k}+b_{k,j,\ell}} - p^{b_{i,j,k}+a_{k,j,\ell}}) + B(p^{a_{\ell,j,i}+b_{k,j,\ell}} - p^{b_{\ell,j,i}+a_{k,j,\ell}}) = 0. \tag{17}$$

We now have two smaller cases:

Case 2.1: consider the case $A \neq B$. Lemma 3.2 gives that there exists a set $\mathscr{D}$ (depending only on p, A, and B) of size at most $\exp(4 \times 18^9) + 1$ such that

$$(a_{\ell,j,i} + b_{k,j,\ell} - b_{\ell,j,i} - a_{k,j,\ell}) - (a_{i,j,k} + b_{k,j,\ell} - b_{i,j,k} - a_{k,j,\ell}) = \Delta$$

belongs to $\mathscr{D}$. We choose $J(i,j,k,\ell) = \mathscr{D}$ in this case.

Case 2.2: consider the case $A = B$. We have that:

$$\frac{x_{m_{i,j,k}}}{x_{m_{\ell,j,i}}} \in u^{A-B}\bar{\mathbb{F}}_p^* = \bar{\mathbb{F}}_p^* \tag{18}$$

From (14) and (18), we have:

$$x_{m_{\ell,j,i}}^{p^{a_{i,j,k}}+p^{a_{\ell,j,i}}} x_{m_{k,j,\ell}}^{p^{a_{k,j,\ell}}} \in \bar{\mathbb{F}}_p^* \tag{19}$$

This implies that $x_{m_{k,j,\ell}} \in \Gamma$ and $x_{m_{k,j,\ell}} \notin \bar{\mathbb{F}}_p^*$. Hence there is a non-zero integer C (not divisible by p) such that $x_{m_{k,j,\ell}}u^{-C} \in \bar{\mathbb{F}}_p^*$. And (19) yields:

$$B(p^{a_{i,j,k}} + p^{a_{\ell,j,i}}) + Cp^{a_{k,j,\ell}} = 0 \tag{20}$$

By similar arguments for t' using (15), we have:

$$B(p^{b_{i,j,k}} + p^{b_{\ell,j,i}}) + Cp^{b_{k,j,\ell}} = 0 \tag{21}$$

By (20) and (21), we have that

$$(p^{a_{i,j,k}-a_{\ell,j,i}}, p^{a_{k,j,\ell}-a_{\ell,j,i}}) \qquad \text{and} \qquad (p^{b_{i,j,k}-b_{\ell,j,i}}, p^{b_{k,j,\ell}-b_{\ell,j,i}})$$

are solutions of the unit equation $-X - \frac{C}{B}Y = 1$. By Proposition 2.1, there are at most $\exp(3 \times 12^6)$ possibilities (depending only on p, B, and C) for each of $a_{i,j,k} - a_{\ell,j,i}$ and $b_{i,j,k} - b_{\ell,j,i}$. Hence there are at most $\exp(6 \times 12^6)$ possibilities for Δ. We choose $J(i,j,k,\ell)$ to be the set of such possibilities.

In any case, we have that $J(i,j,k,\ell)$ does not depend on t' and has at most $\exp(4 \times 18^9) + 1$ elements. This finishes the proof. $\square$

The next technical result is the key step towards the proof of Theorem 3.3. Recall that $q(L) = p^\lambda$.

Proposition 3.8. *Let* $\mathbf{m} := (m_{i,j,k}) \in \{1, \dots, M\}^{\mathscr{T}(d)}$ *such that* $T_{\mathbf{m}} \neq \emptyset$ *and* $X_{\mathbf{m}} \neq \emptyset$. *Fix* $(i_0, j_0, k_0) \in T_{\mathbf{m}}$ *and* $t \in X_{\mathbf{m}}$ *with*

$$(t_{(i)} - t_{(j)})/(t_{(k)} - t_{(j)}) = x_{m_{i,j,k}}^{p^{a_{i,j,k}}}$$

for every $(i,j,k) \in \mathscr{T}(d)$ *for some sequence of non-negative integers* $\mathbf{a} = (a_{i,j,k})$. *There exists a set* $I \subseteq \mathbb{Z}$ *(possibly depending on* $\mathbf{m}$, t, $\mathbf{a}$, *and* (i_0, j_0, k_0)*) such that the following hold:*

(a) $|I| \leq d^3\lambda + 2d^8 \exp(8 \times 18^9)$.
(b) *For every* $t' \in X_{\mathbf{m}}$, *there exists a sequence* $(b_{i,j,k})$ *of non-negative integers satisfying the two conditions:*
  (i) $(t'_{(i)} - t'_{(j)})/(t'_{(k)} - t'_{(j)}) = x_{m_{i,j,k}}^{p^{b_{i,j,k}}}$ *for every* $(i,j,k) \in \mathscr{T}(d)$.
  (ii) $(b_{i,j,k} - a_{i,j,k}) - (b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0}) \in I$ *for any* $(i,j,k) \in \mathscr{T}(d)$.

Proof. Let $t' \in X_{\mathbf{m}}$. By the definition of $X_{\mathbf{m}}$, we can choose a sequence $(c_{j,i,k})$ of non-negative integers such that

$$(t'_{(i)} - t'_{(j)})/(t'_{(k)} - t_{(j)}) = x_{m_{i,j,k}}^{p^{c_{i,j,k}}}$$

for every $(i,j,k) \in \mathscr{T}(d)$. The goal is to modify the sequence $(c_{i,j,k})$ into the sequence $(b_{i,j,k})$ such that for any $(i,j,k) \in \mathscr{T}(d)$, the number $(b_{i,j,k} - a_{i,j,k}) - (b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0})$ lies in a set I independent of t' whose size is at most the given bound.

Recall that for $(i,j,k) \in T_{\mathbf{m}}$, the value of $b_{i,j,k}$ is uniquely determined and is equal to $c_{i,j,k}$. For $(i,j,k) \in \mathscr{T}(d) \setminus T_{\mathbf{m}}$, we have that $x_{m_{i,j,k}} \in \bar{\mathbb{F}}_p^* \cap L^* = \mathbb{F}_{q(L)}^*$, hence $x_{m_{i,j,k}}^{p^\lambda} = x_{m_{i,j,k}}$. This allows us to replace $c_{i,j,k}$ by $c_{i,j,k} + \omega\lambda$ for any integer ω. We now define $b_{i,j,k}$ as follows. Let $\gamma_{i,j,k}$ be the smallest non-negative integer satisfying:

$$-a_{i_0,j_0,k_0} + a_{i,j,k} + \gamma_{i,j,k}\lambda \geq 0.$$

We now let $b_{i,j,k}$ to be of the form $c_{i,j,k} + \omega\lambda$ for some integer ω such that:

$$b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0} + a_{i,j,k} + \gamma_{i,j,k}\lambda \leq b_{i,j,k} < b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0} + a_{i,j,k} + (\gamma_{i,j,k}+1)\lambda.$$

For $(i,j,k) \in \mathscr{T}(d)$, denote $\Delta_{i,j,k} := b_{i,j,k} - a_{i,j,k}$. The bottom line of the above definition of $\gamma_{i,j,k}$ and $b_{i,j,k}$ is that the following properties hold for every $(i,j,k) \in \mathscr{T}(d) \setminus T_{\mathbf{m}}$:

$$\gamma_{i,j,k} \text{ does not depend on } t'; \tag{22}$$

$$b_{i,j,k} \text{ is non-negative;} \tag{23}$$

$$\gamma_{i,j,k}\lambda \leq \Delta_{i,j,k} - \Delta_{i_0,j_0,k_0} < (\gamma_{i,j,k}+1)\lambda. \tag{24}$$

Define $I_1 = \bigcup_{(i,j,k) \in \mathscr{T}(d) \setminus T_{\mathbf{m}}} \{\alpha \in \mathbb{Z} : \gamma_{i,j,k}\lambda \leq \alpha < (\gamma_{i,j,k}+1)\lambda\}$. Let J be the set of size at most $d^4(\exp(4 \times 18^9) + 1)$ as in Proposition 3.7 and define $I_2 := \{\alpha + \beta : \alpha, \beta \in J\}$. We now define:

$$I := \{0\} \cup I_1 \cup I_2$$

which gives that:

$$|I| \leq 1 + d(d-1)(d-2)\lambda + d^8(\exp(4 \times 18^9) + 1)^2 < d^3\lambda + 2d^8 \exp(8 \times 18^9).$$

We need to prove:

$$\Delta_{i,j,k} - \Delta_{i_0,j_0,k_0} \in I \text{ for every } (i,j,k) \in \mathscr{T}(d). \tag{25}$$

This holds trivially when $(i,j,k) = (i_0,j_0,k_0)$. By (24), we have that (25) holds when $(i,j,k) \in \mathscr{T}(d) \setminus T_{\mathbf{m}}$. It remains to consider $(i,j,k) \in T_{\mathbf{m}}$ and $(i,j,k) \neq (i_0,j_0,k_0)$. Since $\mathrm{Gal}(L/K)$ acts transitively on the set $\{t'_{(1)},\dots,t'_{(d)}\}$, we can find $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(t'_{(j)}) = t'_{(j_0)}$ and let $i_1,k_1 \in \{1,\dots,d\}$ such that $\sigma(t'_{(i)}) = t'_{(i_1)}$ and $\sigma(t'_{(k)}) = t'_{(k_1)}$. By Lemma 3.6, we have:

$$\Delta_{i,j,k} - \Delta_{i_0,j_0,k_0} = \Delta_{i_1,j_0,k_1} - \Delta_{i_0,j_0,k_0}. \tag{26}$$

If $(i_1,j_0,k_0) \in T_{\mathbf{m}}$ then Proposition 3.7 and part (a) of Lemma 3.6 give:

$$\Delta_{i_1,j_0,k_1} - \Delta_{i_0,j_0,k_0} = (\Delta_{i_1,j_0,k_1} - \Delta_{i_1,j_0,k_0}) + (\Delta_{i_1,j_0,k_0} - \Delta_{i_0,j_0,k_0}) \in I_2.$$

The case when $(i_0,j_0,k_1) \in T_{\mathbf{m}}$ is handled similarly. The only case left is that both $x_{m_{i_1,j_0,k_0}}$ and $x_{m_{i_0,j_0,k_1}}$ are in $\bar{\mathbb{F}}_p^*$. In this case, we have:

$$\alpha := \frac{t_{(i_1)} - t_{(j_0)}}{t_{(k_0)} - t_{(j_0)}};\ \beta := \frac{t_{(i_0)} - t_{(j_0)}}{t_{(k_1)} - t_{(j_0)}}$$

$$\alpha' := \frac{t'_{(i_1)} - t'_{(j_0)}}{t'_{(k_0)} - t'_{(j_0)}};\ \beta' := \frac{t'_{(i_0)} - t'_{(j_0)}}{t'_{(k_1)} - t'_{(j_0)}}$$

are all contained in $\bar{\mathbb{F}}_p^*$. Since

$$\frac{t_{(i_1)} - t_{(j_0)}}{t_{(k_1)} - t_{(j_0)}} = \alpha\beta \frac{t_{(k_0)} - t_{(j_0)}}{t_{(i_0)} - t_{(j_0)}}$$

$$\frac{t'_{(i_1)} - t'_{(j_0)}}{t'_{(k_1)} - t'_{(j_0)}} = \alpha'\beta' \frac{t'_{(k_0)} - t'_{(j_0)}}{t'_{(i_0)} - t'_{(j_0)}}$$

we have

$$x_{m_{i_1,j_0,k_1}}^{p^{a_{i_1,j_0,k_1}}} = \alpha\beta x_{m_{k_0,j_0,i_0}}^{p^{a_{k_0,j_0,i_0}}} \tag{27}$$

$$x_{m_{i_1,j_0,k_1}}^{p^{b_{i_1,j_0,k_1}}} = \alpha'\beta' x_{m_{k_0,j_0,i_0}}^{p^{b_{k_0,j_0,i_0}}}. \tag{28}$$

Hence the radical in L of the group generated by $x_{m_{i_1,j_0,k_1}}$ and $x_{m_{k_0,j_0,i_0}}$ has rank one. As in the proof of Proposition 3.7, there exist $u \in L^* \setminus \bar{\mathbb{F}}_p^*$ and non-zero integers A, B such that $x_{m_{i_1,j_0,k_1}} u^{-A}$ and $x_{m_{k_0,j_0,i_0}} u^{-B}$ are in $\bar{\mathbb{F}}_p^*$. Together with equations (27) and (28), we have $Ap^{a_{i_1,j_0,k_1}} = Bp^{a_{k_0,j_0,i_0}}$ and $Ap^{b_{i_1,j_0,k_1}} = Bp^{b_{k_0,j_0,i_0}}$. This and part (a) of Lemma 3.6 give $\Delta_{i_1,j_0,k_1} - \Delta_{i_0,j_0,k_0} = 0 \in I$. This finishes the proof. □

Let $\mathbf{m} = (m_{i,j,k}) \in \{1,\dots,M\}^{\mathscr{T}(d)}$ such that $T_{\mathbf{m}} \neq \emptyset$ and $X_{\mathbf{m}} \neq \emptyset$. Fix $(i_0,j_0,k_0) \in T_{\mathbf{m}}$ and $t \in X_{\mathbf{m}}$ with:

$$\frac{t_{(i)} - t_{(j)}}{t_{(k)} - t_{(j)}} = x_{m_{i,j,k}}^{p^{a_{i,j,k}}}$$

for every $(i,j,k) \in \mathscr{T}(d)$ for some sequence of non-negative integers $(a_{i,j,k})$. Let $I_{\mathbf{m}}$ denote the resulting set as in the conclusion of Proposition 3.8.

For every $\mathbf{D} := (D_{i,j,k}) \in I_{\mathbf{m}}^{\mathscr{T}(d)}$, define $X_{\mathbf{m},\mathbf{D}}$ to be the set of $t' \in X_{\mathbf{m}}$ such that there exists an integer C satisfying the following:

$$\frac{t'_{(i)} - t'_{(j)}}{t'_{(k)} - t'_{(j)}} = x_{m_{i,j,k}}^{p^{C+D_{i,j,k}+a_{i,j,k}}} \text{ for every } (i,j,k) \in \mathscr{T}(d). \tag{29}$$

We have:

Lemma 3.9. *Notation as above, we have* $X_{\mathbf{m}} = \bigcup_{\mathbf{D} \in I_{\mathbf{m}}^{\mathscr{T}(d)}} X_{\mathbf{m},\mathbf{D}}$.

Proof. Given $t' \in X_{\mathbf{m}}$, by Proposition 3.8, there is a sequence $(b_{i,j,k})$ such that the following holds:

(i) $\dfrac{t'_{(i)} - t'_{(j)}}{t'_{(k)} - t'_{(j)}} = x_{m_{i,j,k}}^{p^{b_{i,j,k}}}$ for every $(i,j,k) \in \mathscr{T}(d)$.

(ii) $D_{i,j,k} := (b_{i,j,k} - a_{i,j,k}) - (b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0}) \in I_{\mathbf{m}}$ for every $(i,j,k) \in \mathscr{T}(d)$.

Let $\mathbf{D} = (D_{i,j,k})$, we have $t' \in X_{\mathbf{m},\mathbf{D}}$ (by taking $C := b_{i_0,j_0,k_0} - a_{i_0,j_0,k_0}$). □

For every $z \in X_{\mathbf{m},\mathbf{D}}$, define $e(z)$ to be the largest non-negative integer n such that

$$\frac{z_{(i_0)} - z_{(j_0)}}{z_{(k_0)} - z_{(j_0)}} \in L^{\langle p^n \rangle} := \{\alpha^{p^n} : \alpha \in L\}.$$

Such an n exists since $\dfrac{z_{(i_0)} - z_{(j_0)}}{z_{(k_0)} - z_{(j_0)}}$ is a power of $x_{m_{i_0,j_0,k_0}}$ which is not algebraic over $\mathbb{F}_p$.

If $X_{\mathbf{m},\mathbf{D}} \neq \emptyset$, define $z = z(\mathbf{m},\mathbf{D})$ to be an element of $X_{\mathbf{m},\mathbf{D}}$ such that $e(z)$ is minimal. Let t' be any element in $X_{\mathbf{m},\mathbf{D}}$. By the definition of $X_{\mathbf{m},\mathbf{D}}$, there is an integer C such that:

$$\frac{t'_{(i)} - t'_{(j)}}{t'_{(k)} - t'_{(j)}} = \left(\frac{z_{(i)} - z_{(j)}}{z_{(k)} - z_{(j)}}\right)^{p^C} \text{ for every } (i,j,k) \in \mathscr{T}(d).$$

By the minimality of $e(z)$, we must have that $C \geq 0$. As in the proof of Lemma 3.5, we have that

$$a := \frac{t'_{(i)} - t'_{(j)}}{(z_{(i)} - z_{(j)})^{p^C}}$$

is non-zero and independent of distinct $i,j \in \{1,\ldots,d\}$. Hence $a \in K^*$ since it is invariant under $\mathrm{Gal}(L/K)$. The element $b := t'_{(i)} - a z_{(i)}^{p^C}$ is independent of $i \in \{1,\ldots,d\}$. So it is invariant under $\mathrm{Gal}(L/K)$ and, hence, is in K. Therefore $t' = az^q + b$ with $q = p^C$, $a \in K^*$, and $b \in K$. Since $\mathcal{O}[z] = \mathcal{O}[t'] = \mathcal{O}[s]$, we have that $\mathrm{discr}_K(z)$, $\mathrm{discr}_K(t')$, and $D := \mathrm{discr}_K(s)$ differ (multiplicatively) by a unit. This implies $\dfrac{a^{d(d-1)}}{D^{1-q}} \in \mathcal{O}^*$.

We now finish the proof of Theorem 3.3, as follows. The t_i's in the conclusion of Theorem 3.3 could be taken to be the t_i's in the conclusion of Lemma 3.5 together with the elements $z(\mathbf{m},\mathbf{D})$ from the above discussion. The number of such elements is at most:

$$\left(\min\{q(L), q(K)^{d^3}\}\right)^{d^3} + M^{d(d-1)(d-2)} \left(d^3\lambda + 2d^8 \exp(8 \times 18^9)\right)^{d(d-1)(d-2)}$$

which is less than:

$$\left(\min\{q(L), q(K)^{d^3}\}\right)^{d^3} + \left(\exp(18^{10})p^{2r}d^8\lambda\right)^{d^3}.$$

3.3. **An example.** For the sake of completeness, we construct an example to show that it is not always possible to have $t = at_i^q + b$ as in Theorem 1.2 with the further restriction that b is in $\mathcal{O}$.

Let $\mathcal{O} = \mathbb{F}_2[x]$, $K = \mathbb{F}_2(x)$, and let $\eta \in \mathcal{O} \setminus \mathbb{F}_2$ be a non-constant polynomial such that the following properties hold:

(i) x does not divide η (as polynomials in $\mathbb{F}_2[x]$);
(ii) the polynomial $P(Y) := Y^4 + x^4Y^2 + x^3Y + \eta$ is irreducible over K.

It is easy to check that, for instance, $\eta = x + 1$ satisfies the above conditions. In fact, there are infinitely many such η's.

We now let s be a root of $P(Y)$. Since s is separable over K, we have that $s^{4^m} \neq K$ for every $m \in \mathbb{N}$. The sequence $\{\eta_m\}_{m\in\mathbb{N}}$ of elements of $\mathcal{O}$ is defined recursively as follows:

$$\eta_1 = \eta;\ \eta_{m+1} = \eta^{4^m} + x^{3\cdot 4^m}\eta_m + x^{4^{m+1}}\eta_m^2 \text{ for } m \in \mathbb{N}.$$

For $m \in \mathbb{N}$, define $z_m := \dfrac{s^{4^m} + \eta_m}{x^{4^m-1}}$. Since $\mathrm{discr}_K(s) = x^{12}$, we have that $\mathrm{discr}_K(s) = \mathrm{discr}_K(z_m)$ for every $m \in \mathbb{N}$. We have:

Lemma 3.10. *$\mathcal{O}[s] = \mathcal{O}[z_m]$ for every $m \in \mathbb{N}$.*

Proof. Since $\mathrm{discr}_K(s) = \mathrm{discr}_K(z_m)$, it suffices to show that $z_m \in \mathcal{O}[s]$ for every $m \in \mathbb{N}$. From $P(s) = 0$, we have $z_1 = \dfrac{s^4 + \eta}{x^3} = xs^2 + s \in \mathcal{O}[s]$. We complete the proof by proving that $z_{m+1} \in \mathcal{O}[z_m]$ for every $m \in \mathbb{N}$.

From $P(s)^{4^m} = 0$, we have:

$$\frac{s^{4^{m+1}} + \eta^{4^m}}{x^{4^{m+1}-1}} = xs^{2\cdot 4^m} + \frac{s^{4^m}}{x^{4^m-1}}.$$

Adding $\dfrac{1}{x^{4^{m+1}-1}}\left(x^{3\cdot 4^m}\eta_m + x^{4^{m+1}}\eta_m^2\right)$ to both sides and using the recurrence relation defining $\{\eta_m\}$, we have:

$$z_{m+1} = x\left(s^{4^m} + \eta_m\right)^2 + \frac{s^{4^m} + \eta_m}{x^{4^m-1}} \in \mathcal{O}[z_m].$$

□

Let v denote the discrete valuation on $\mathcal{O}$ such that $v(x) = 1$. We have:

Lemma 3.11. *$v(\eta_{m+1} - \eta_m^4) = 4^{m+1} - 4$ for every $m \in \mathbb{N}$.*

Proof. From $v(\eta_1) = 0$ and $\eta_2 - \eta_1^4 = x^{12}\eta_1 + x^{16}\eta_1^2$, the lemma holds when $m = 1$. Using

$$\eta_{m+1} - \eta_m^4 = x^{3\cdot 4^m}(\eta_m - \eta_{m-1}^4) + x^{4^{m+1}}(\eta_m - \eta_{m-1}^4)^2$$

thanks to the recursive formula for $\{\eta_m\}$ and by induction, the lemma holds for every $m \in \mathbb{N}$. □

The next result shows that we have the desired example:

Proposition 3.12. *There does not exist a finite set $\{t_1, \ldots, t_N\}$ satisfying the following conditions:*

(a) $\mathcal{O}[t_i] = \mathcal{O}[s]$ *for* $1 \leq i \leq N$;
(b) *for every* $m \in \mathbb{N}$, *there exist* $i \in \{1, \ldots, N\}$, *a power* q *of* p, *elements* $a \in K$ *and* $b \in \mathcal{O}$ *such that* $z_m = at_i^q + b$.

Proof. Assume there exists such a finite set. Then there are t such that $\mathcal{O}[t] = \mathcal{O}[s]$ and an infinite subset $\mathcal{M} \subseteq \mathbb{N}$ such that for every $m \in \mathcal{M}$, there are a power q_m of p, $a_m \in K$, and $b_m \in \mathcal{O}$ such that $z_m = a_m t^{q_m} + b_m$. After replacing $\mathcal{M}$ by an infinite subset if necessary, we may assume that $q_m \leq q_n$ for $m, n \in \mathcal{M}$ with $m < n$.

Let j be the smallest element of $\mathcal{M}$, for every $m \in \mathcal{M}$, we can write:

$$z_m = \frac{a_m}{a_j^{q_m/q_j}} \left(a_j t^{q_j} + b_j\right)^{q_m/q_j} + b_m - \frac{a_m}{a_j^{q_m/q_j}} b_j^{q_m/q_j} = c_m z_j^{q_m/q_j} + d_m \tag{30}$$

where $c_m = \dfrac{a_m}{a_j^{q_m/q_j}}$ and $d_m = b_m - \dfrac{a_m}{a_j^{q_m/q_j}} b_j^{q_m/q_j}$. Recall that v is the discrete valuation on $\mathcal{O}$ with $v(x) = 1$. By comparing discriminant, we have $a_m^{12} = \operatorname{discr}_K(s)^{1-q_m}$ and $a_j^{12} = \operatorname{discr}_K(s)^{1-q_j}$. Therefore:

$$\left(\frac{a_m}{a_j^{q_m/q_j}}\right)^{12} = \operatorname{discr}_K(s)^{1-q_m/q_j} = x^{12(1-q_m/q_j)}. \tag{31}$$

Hence $v\left(\dfrac{a_m}{a_j^{q_m/q_j}}\right) = 1 - \dfrac{q_m}{q_j}$. Since $b_m \in \mathcal{O}$ for every $m \in \mathcal{M}$, we have:

$$v(d_m) \geq 1 - \frac{q_m}{q_j} \text{ for } m \in \mathcal{M}. \tag{32}$$

We can rewrite (30) as:

$$\frac{s^{4^m} + \eta_m}{x^{4^m - 1}} = c_m \left(\frac{s^{4^j} + \eta_j}{x^{4^j - 1}}\right)^{q_m/q_j} + d_m. \tag{33}$$

Claim: $\dfrac{q_m}{q_j} = 4^{m-j}$ and $\dfrac{c_m}{x^{(4^j-1)q_m/q_j}} = \dfrac{1}{x^{4^m-1}}$. Let σ be a nontrivial embedding of $K(s)$ into $\bar{K}$. Applying σ to (33) and take the difference, we have:

$$\frac{(s - \sigma(s))^{4^m}}{x^{4^m-1}} = \frac{c_m}{x^{(4^j-1)q_m/q_j}} (s - \sigma(s))^{4^j q_m/q_j}. \tag{34}$$

Consequently:

$$(s - \sigma(s))^{4^m - 4^j q_m/q_j} = c_m x^{4^m - 1 - (4^j - 1)q_m/q_j} \tag{35}$$

Raising to the 12-th power and using (31), we have:

$$(s - \sigma(s))^{12(4^m - 4^j q_m/q_j)} = x^{12(4^m - 4^j q_m/q_j)}.$$

If $4^m - 4^j q_m/q_j \neq 0$ then $s - \sigma(s) = \zeta x$ for some $\zeta \in \bar{\mathbb{F}}_2^*$, hence $0 = P(s) - P(\sigma(s)) = \zeta^4 x^4 + \zeta^2 x^6 + \zeta x^4$ which is impossible. Therefore we must have $4^m - 4^j q_m/q_j = 0$, or $q_m/q_j = 4^{m-j}$. Together with (33), we have:

$$\left(\frac{c_m}{x^{(4^j-1)q_m/q_j}} - \frac{1}{x^{4^m-1}}\right) s^{4^m} \in K.$$

Since $s^{4^m} \notin K$, we must have $\dfrac{c_m}{x^{(4^j-1)q_m/q_j}} - \dfrac{1}{x^{4^m-1}} = 0$. This proves the claim.

From (33) and the claim above, we have:

$$\frac{\eta_m}{x^{4^m-1}} = \frac{\eta_j^{4^{m-j}}}{x^{4^m-1}} + d_m \text{ for } m \in \mathcal{M}. \tag{36}$$

Applying Lemma 3.11 repeatedly, we have $v(\eta_m - \eta_j^{4^{m-j}}) = 4^{j+1} - 4$. On the other hand, (32) gives that $v(x^{4^m-1}d_m) \geq 4^m - 1 + 1 - 4^{m-j} = 4^m - 4^{m-j}$. Together with (36), we have $4^{j+1} - 4 \geq 4^m - 4^{m-j}$. This gives a contradiction when m is sufficiently large. □

3.4. **Proof of Corollary 1.4.** Notation as in Corollary 1.4, there are at most $N(d)$ subextensions F/K of E/K. For every such F/K, let $X(F)$ be the set of elements $t \in E$ integral over $\mathcal{O}_{K,T}$ such that $\mathrm{discr}_K(t) \in \mathcal{O}_{K,T}^*$ *and* $K(t) = F$. If $X(F) \neq \emptyset$, pick an element $s \in X(F)$. We have that $t \in X(F)$ if and only if $\mathcal{O}_{K,T}[t] = \mathcal{O}_{K,T}[s]$. Theorem 1.2 gives that there are at most

$$q(K)^{d^6} + \Big(\exp(18^{10})p^{3d^4|T|}\log_p q(K)\Big)^{d^3}$$

elements $t_1, \ldots, t_N \in X(F)$ such that every $t \in X(F)$ has the form $at_i^q + b$ for some $1 \leq i \leq N$, power $q \geq 1$ of p, $a \in K^*$, and $b \in K$. By comparing discriminant, we have that $a^{d(d-1)} \in \mathcal{O}_{K,T}^*$, hence $a \in \mathcal{O}_{K,T}^*$. Therefore $b \in \mathcal{O}_{K,T}$ and this finishes the proof.

4. Proof of Theorem 1.10

4.1. **Notation and preliminary results.** Throughout this section, assume the notation in Theorem 1.10. Recall the condition that $\{s^n, t^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ (see Section 5). Let L be the Galois closure of $K(s,t)/K$ and let G denote the radical in L of the group generated by $\mathcal{O}^*$ and all the conjugates of s and t. Let r denote the rank of G. Define e (respectively f) to be the smallest integer in $\mathbb{N}$ such that $K(s^e) \subseteq K(s^n)$ (respectively $K(t^f) \subseteq K(t^n)$) for every $n \in \mathbb{N}$; in other words, $K(s^e) = \cap_{n\in\mathbb{N}} K(s^n)$ (respectively $K(t^f) = \cap_{n\in\mathbb{N}} K(t^n)$). For every $1 \leq k \leq e$ and $1 \leq \ell \leq f$, define the set:

$$\mathcal{M}(k,\ell) := \{(m,n) \in \mathcal{M}(\mathcal{O},s,t) : \ m \equiv k \bmod e, \ n \equiv \ell \bmod f\}.$$

As in the proof of Theorem 1.2, if $\mathcal{O}[s^m] = \mathcal{O}[t^n]$ and $\sigma\,\mathrm{Gal}(L/K(s^m))$ is a non-identity coset of $\mathrm{Gal}(L/K(s^m))$ in $\mathrm{Gal}(L/K)$, then

$$u_{m,n,\sigma} := \frac{s^m - \sigma(s^m)}{t^n - \sigma(t^n)}$$

is a unit in the ring $\mathcal{O}[s^m, \sigma(s^m)]$.

Lemma 4.1. *We have the following:*

(a) *for every $(m,n) \in \mathcal{M}(\mathcal{O},s,t)$, we have $(pm,pn) \in \mathcal{M}(\mathcal{O},s,t)$;*
(b) $\gcd(e,p) = \gcd(f,p) = 1$*;*
(c) *there is a power $q_1 > 1$ of p such that for every $(m,n) \in \mathcal{M}(k,\ell)$, we have $(q_1 m, q_1 n) \in \mathcal{M}(k,\ell)$.*

Proof. Part (a) follows from the easy fact that if $\mathcal{O}[s^m] = \mathcal{O}[t^n]$ then $\mathcal{O}[s^{pm}] = \mathcal{O}[t^{pn}]$.

We prove $\gcd(e,p) = 1$ by contradiction, the identity $\gcd(f,p) = 1$ could be proved by similar arguments. Assume $e = p\alpha$ with $\alpha \in \mathbb{N}$. By the minimality of e, we have that $K(s^\alpha)$ strictly contains $K(s^e)$. Pick $\tau \in \mathrm{Gal}(L/K(s^e))$ outside

$\mathrm{Gal}(L/K(s^\alpha))$. We have: $(s/\tau(s))^e = 1$, hence $(s/\tau(s))^\alpha = 1$ since $e = p\alpha$. Hence τ fixes s^α, contradiction. This proves part (b).

For part (c), we choose q_1 such that $q_1 k \equiv k$ modulo e and $q_1 \ell \equiv \ell$ modulo f. This is possible by part (b). □

Definition 4.2. *We have the following definitions.*

(a) *Let $M \in \mathbb{N}$, $\mathbf{x} \in \mathbb{N}^M$, and $q > 1$ be a power of p. The q-Frobenius subset of $\mathbb{N}^M$ generated by $\mathbf{x}$ is defined to be:*

$$F_1(q; \mathbf{x}) := \{q^k \mathbf{x} : \ k \in \mathbb{N}_0\}.$$

(b) *Let $(a, b) \in \mathbb{N}^2$, the doubly q-Frobenius subset of $\mathbb{N}^2$ generated by (a, b) is defined to be:*

$$F_2(q; a, b) := \{(q^i a, q^j b) : \ i, j \in \mathbb{N}_0\}.$$

We say that q is the base *of $F_1(q; \mathbf{x})$ and $F_2(q; a, b)$. A Frobenius subset of $\mathbb{N}^M$ (respectively doubly Frobenius subset of $\mathbb{N}^2$) is a set of the form $F_1(q; \mathbf{x})$ (respectively $F_2(q; a, b)$).*

Remark 4.3. Sets of the form $F(q; a_1, a_2, a_3, a_4)$ as defined in Definition 1.8 include Frobenius subsets of $\mathbb{N}^2$ (when $a_2 = a_4 = 0$) and doubly Frobenius subsets of $\mathbb{N}^2$ (when $a_2 = a_3 = 0$) as special cases.

Our proof of Theorem 1.10 will be divided into two cases.

4.2. **The case when $K(s^e) \neq K(t^f)$.** In this subsection, we prove the following:

Proposition 4.4. *Let s and t be as in Theorem 1.10. Assume that $K(s^e) \neq K(t^f)$. Then the set $\mathcal{M} := \mathcal{M}(\mathcal{O}, s, t)$ is a finite union of Frobenius and doubly Frobenius subsets of $\mathbb{N}^2$.*

We start with an easy lemma:

Lemma 4.5. *Let $r \in \mathbb{N}$ and let Z be a nonempty subset of $\mathbb{N}^k$. Assume that Z is contained in a finite union of Frobenius subsets of $\mathbb{N}^k$ and there is $q > 1$ which is a power of p such that $qZ \subset Z$. Then Z is a finite union of Frobenius subsets of base q.*

Proof. We may assume that Z is contained in a finite disjoint union of Frobenius subsets of $\mathbb{N}$ whose bases are powers of q. Denote these Frobenius subsets by $F_1, \ldots, F_n$. We may assume $Z \cap F_i \neq \emptyset$ and let $\mathbf{x}_i$ be the minimal element in $Z \cap F_i$ for $1 \leq i \leq n$. Then we have:

$$Z = \bigcup_{i=1}^{n} \{q^n \mathbf{x}_i : \ n \in \mathbb{N}_0\}.$$

□

We have the following:

Proposition 4.6. *There is a constant C_1 such that the following hold.*

(a) *For every $m \in \pi_1(\mathcal{M})$, for every subset of at least C_1 elements in*

$$\mathcal{M}_1(m) := \{n \in \mathbb{N} : \ (m, n) \in \mathcal{M}\}$$

there exist $n_1 < n_2$ such that $\dfrac{n_2}{n_1}$ is a power of p.

(b) *For every $n \in \pi_2(\mathcal{M})$, for every subset of at least C_1 elements in*

$$\mathcal{M}_2(n) := \{m \in \mathbb{N} : \ (m,n) \in \mathcal{M}\}$$

there exist $m_1 < m_2$ in $\mathcal{M}_2(n)$ such that $\dfrac{m_2}{m_1}$ is a power of p.

Proof. It suffices to prove (a) only since (b) is completely analogous. Since $t^k \notin \mathcal{O}$ for every $k \in \mathbb{N}$, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that σ does not fix t^k for every $k \in \mathbb{N}$. Recall that when $(m,n) \in \mathcal{M}$, we have that $u_{m,n,\sigma} := \dfrac{s^m - \sigma(s^m)}{t^n - \sigma(t^n)}$ is an element of G.

Let Γ be the group generated by G and $s^m - \sigma(s^m)$. Hence the rank of Γ is at most $r+1$. We have that $u_{m,n,\sigma}(t^n/(s^m - \sigma(s^m)), -\sigma(t^n)/(s^m - \sigma(s^m)))$ gives a solution of $x + y = 1$ with $(x,y) \in \Gamma^2$. By Proposition 2.6, there is a finite subset $\mathscr{X}$ of L^* such that $|\mathscr{X}| \le p^{2r+2}$ and

$$\frac{t^n}{\sigma(t^n)} = u^{q^\alpha}$$

for some $u \in \mathscr{X}$ and $\alpha \in \mathbb{N}_0$.

Now we can take $C_1 = p^{2r+2} + 1$. For any C_1 distinct elements of $\mathcal{M}_1(m)$, there are two elements $n_1 < n_2$ such that there exist $u \in X$ and $\alpha_1 < \alpha_2$ such that

$$\frac{t^{n_1}}{\sigma(t^{n_1})} = u^{p^{\alpha_1}} \text{ and } \frac{t^{n_2}}{\sigma(t^{n_2})} = u^{p^{\alpha_2}}.$$

Note that $\frac{t}{\sigma(t)} \notin \bar{\mathbb{F}}_p^*$ since σ does not fix any power of t. Hence $n_1 p^{\alpha_2} = n_2 p^{\alpha_1}$. □

Proposition 4.7. *The following results hold.*

(a) *If $K(s^e) \not\subseteq K(t^f)$ then the set $\pi_1(\mathcal{M})$ is a finite union of p-Frobenius subsets of $\mathbb{N}$.*
(b) *If $K(t^f) \not\subseteq K(s^e)$ then the set $\pi_2(\mathcal{M})$ is a finite union of p-Frobenius subsets of $\mathbb{N}$.*

Proof. It suffices to prove (a) only. There exists $\sigma \in \mathrm{Gal}(L/K(t^f))$ such that $\sigma \notin \mathrm{Gal}(L/K(s^e))$. For every $1 \le \ell \le f$, define $\mathcal{M}(\cdot,\ell) := \{(m,n) \in \mathcal{M} : \ n \equiv \ell \bmod f\}$. By our assumption, we have $\mathcal{M}(\cdot,f) = \emptyset$.

Fix any $1 \le \ell < f$, let $(m,n) \in \mathcal{M}(\cdot,\ell)$, and write $n = \tilde{n}f + \ell$. As before, we have $u_{m,n,\sigma} \in G$ such that:

$$0 \ne s^m - \sigma(s^m) = u_{m,n,\sigma}(t^n - \sigma(t^n)) = u_{m,n,\sigma} t^{\tilde{n}f}(t^\ell - \sigma(t^\ell)).$$

Let Γ be the group generated by G and $t^\ell - \sigma(t^\ell)$ whose rank is at most $r+1$. The above identity gives that $\dfrac{1}{u_{m,n,\sigma} t^{\tilde{n}f}(t^\ell - \sigma(t^\ell))}(s^m, -\sigma(s^m))$ is a solution of the equation $x + y = 1$ with $(x,y) \in G^2$. Note that $\dfrac{s}{\sigma(s)} \notin \bar{\mathbb{F}}_p^*$ since σ cannot fix any power of s. Write $C_2 = p^{2r+2} + 1$. By using Proposition 2.6 as in the proof of Proposition 4.6, we have that for every subset of at least C_2 elements of $\pi_1(W(\cdot,\ell))$, there exist $m_1 < m_2$ such that $\dfrac{m_2}{m_1}$ is a power of p. Hence the same conclusion holds for every subset of at least fC_2 elements of $\pi_1(W)$. By Lemma 4.1, if $m \in \pi_1(\mathcal{M})$ then $pm \in \pi_1(\mathcal{M})$. This implies that $\pi(W)$ is the union of at most fC_2 many p-Frobenius subsets. □

Proof of Proposition 4.4. We may assume $K(s^e) \nsubseteq K(t^f)$ since the case $K(t^f) \nsubseteq K(s^e)$ is similar. By Proposition 4.7, the set $\pi_1(\mathcal{M})$ is a (disjoint) union of finitely many p-Frobenius subsets $F_1, \ldots, F_k$ of $\mathbb{N}$. Fix any i such that $1 \leq i \leq k$, it suffices to show that the set:

$$\mathcal{M} \cap F_i \times \mathbb{N} = \{(m,n) \in \mathcal{M} : \ m \in F_i\}$$

is contained in finitely many Frobenius and doubly Frobenius subsets *of* $\mathcal{M}$.

Recall the notation $\mathcal{M}_1(m)$ and the constant C_1 in Proposition 4.6. There are two cases:

Case 1: $\{|\mathcal{M}_1(m)| : \ m \in F_i\}$ is bounded. Let $m_i \in F_i$ be such that $M := |\mathcal{M}_1(m_i)| = \max\{|\mathcal{M}_1(m)| : \ m \in F_i\}$. Denote $\mathcal{M}_1(m_i) := \{n_1, \ldots, n_M\}$. For every $m \in F_i$ satisfying $m > m_i$, write $m = p^v m_i$ for some $v \in \mathbb{N}$. By Lemma 4.1 and the maximality of $|\mathcal{M}_1(m_i)|$, we conclude that:

$$\mathcal{M}_1(m) = \{p^v n_1, \ldots, p^v n_M\}.$$

Hence the set $\{(m,n) \in \mathcal{M} \cap F_i \times \mathbb{N} : \ m \geq m_i\}$ is a finite union of p-Frobenius subsets. The set $\{(m,n) \in \mathcal{M} \cap F_i \times \mathbb{N} : \ m < m_i\}$ is finite by our assumption in this case, hence, by Lemma 4.1, it is contained in a finite union of Frobenius subsets of $\mathcal{M} \cap F_i \times \mathbb{N}$. Overall, we have that $\mathcal{M} \cap F_i \times \mathbb{N}$ is a finite union of its Frobenius subsets.

Case 2: $\{|\mathcal{M}_1(m)| : \ m \in F_i\}$ is unbounded. Hence there exists $\tilde{m} \in F_i$, chosen to be minimal, such that $|\mathcal{M}_1(\tilde{m})| > C_1$. By Proposition 4.6, there are $n_1 < n_2$ in $\mathcal{M}_1(\tilde{m})$ such that $q := \dfrac{n_2}{n_1}$ is a power of p. This implies $\mathcal{O}[s^{\tilde{m}}] = \mathcal{O}[t^{n_1}] = \mathcal{O}[t^{n_2}] = \mathcal{O}[t^{n_1 q}] = \mathcal{O}[s^{\tilde{m}q}]$.

Hence for every $n \in \mathcal{M}_1(\tilde{m})$, we have $\mathcal{O}[t^{nq}] = \mathcal{O}[s^{\tilde{m}q}] = \mathcal{O}[s^{\tilde{m}}]$ which gives that $nq \in \mathcal{M}_1(\tilde{m})$. By Proposition 4.7 and Lemma 4.5, $\mathcal{M}_1(\tilde{m})$ is a finite union of Frobenius subsets of base q. Since $\mathcal{O}[s^{\tilde{m}}] = \mathcal{O}[s^{\tilde{m}q}]$, we have that $\mathcal{M}_1(\tilde{m}) = \mathcal{M}_1(\tilde{m}q^v)$ for every $v \in \mathbb{N}$. Therefore, the set:

$$\{(m,n) \in \mathcal{M} \cap F_i \times \mathbb{N} : \ m = \tilde{m}q^v \text{ for some } v \in \mathbb{N}_0\}$$

is a finite union of doubly Frobenius subsets (of base q).

Write $q = p^w$ for some $w \in \mathbb{N}$. For $1 \leq j \leq w-1$, by Lemma 4.1, the set $\mathcal{M}_1(\tilde{m}p^j)$ has two elements whose quotient is q since the same holds for $\mathcal{M}_1(\tilde{m})$. Hence we repeat the same arguments where $\tilde{m}$ is replaced by $\tilde{m}p^j$ to conclude that the set:

$$\{(m,n) \in \mathcal{M} \cap F_i \times \mathbb{N} : \ m = \tilde{m}p^j q^v \text{ for some } v \in \mathbb{N}_0\}$$

is a finite union of doubly Frobenius subsets (of base q).

Finally, by the minimality of $\tilde{m}$, the set

$$\{(m,n) \in \mathcal{M} \cap F_i \times \mathbb{N} : m < \tilde{m}\}$$

is finite. By Lemma 4.1, this set is contained in a finite union of Frobenius subsets of $\mathcal{M} \cap F_i \times \mathbb{N}$.

Overall, we conclude that $\mathcal{M} \cap F_i \times \mathbb{N}$ is a finite union of Frobenius and doubly Frobenius subsets. This finishes the proof. □

4.3. **The case when $K(s^e) = K(t^f)$.** We now assume that $K(s^e) = K(t^f)$ and denote this field by K^o. Note that $K \subsetneq K^o$ by the assumption on s and t. For $1 \le k \le e$ and $1 \le \ell \le f$, consider the set $\mathcal{M}(k,\ell) = \{(m,n) \in \mathcal{M}(\mathcal{O},s,t) : m \equiv k \bmod e,\ n \equiv \ell \bmod f\}$. The convenience of doing this is that we can fix $F := K(s^k) = K(s^m) = K(t^n) = K(t^\ell)$ for $(m,n) \in \mathcal{M}(k,\ell)$. We have the tower of fields:

$$K \subsetneq K^o \subset F \subset L.$$

As before, for every $(m,n) \in \mathcal{M}(k,\ell)$ and $\sigma \in \mathrm{Gal}(L/K) \setminus \mathrm{Gal}(L/F)$ there is $u_{m,n,\sigma} \in G$ such that $0 \ne s^m - \sigma(s^m) = u_{m,n,\sigma}(t^n - \sigma(t^n))$. Therefore $\mathbf{x}_{m,n,\sigma} := \left(\dfrac{s^m}{\sigma(s^m)}, -\dfrac{u_{m,n,\sigma}t^n}{\sigma(s^m)}, \dfrac{u_{m,n,\sigma}\sigma(t^n)}{\sigma(s^m)}\right)$ is a solution of the unit equation

$$x + y + z = 1 \text{ with } (x,y,z) \in G^3. \tag{37}$$

Note that $\mathbf{x}_{m,n,\sigma} = \mathbf{x}_{m,n,\tau}$ and $u_{m,n,\sigma} = u_{m,n,\tau}$ if the two cosets $\sigma\,\mathrm{Gal}(L/F)$ and $\tau\,\mathrm{Gal}(L/F)$ coincide. We have the following:

Proposition 4.8. *The set of $(m,n) \in \mathcal{M}(\mathcal{O},s,t)$ such that $\mathbf{x}_{m,n,\sigma}$ is degenerate for every coset $\sigma\,\mathrm{Gal}(L/F)$ with $\sigma \notin \mathrm{Gal}(L/K^o)$ is contained in $\mathcal{A}(\mathcal{O},s,t) \cup \mathcal{B}(\mathcal{O},s,t) \cup \mathcal{C}(\mathcal{O},s,t)$.*

Proof. A proof in the characteristic zero case is given in [Ngu15, pp. 12–14]. The same proof can be used for positive characteristic. □

By Proposition 4.8, to finish the proof of Theorem 1.10, we show that for every $\sigma \in \mathrm{Gal}(L/K) \setminus \mathrm{Gal}(L/K^o)$, the set:

$$\mathcal{M}(k,\ell,\sigma) := \{(m,n) \in \mathcal{M}(k,\ell) :\ \mathbf{x}_{m,n,\sigma} \text{ is nondegenerate}\}$$

is contained in a finite union of sets of the form $F(q;c_1,c_2,c_3,c_4)$. We have:

Lemma 4.9. *There is a power $q_1 > 1$ of p such that $(q_1 m, q_1 n) \in \mathcal{M}(k,\ell,\sigma)$ whenever $(m,n) \in \mathcal{M}(k,\ell,\sigma)$.*

Proof. This follows from part (c) of Lemma 4.1 and the fact that $x_{q_1 m,q_1 n,\sigma}$ is degenerate iff $x_{m,n,\sigma}$ is degenerate. □

Since $\sigma \notin \mathrm{Gal}(L/K^o)$, it does not fix s^n or t^n for any $n \in \mathbb{N}$. In other words, $\dfrac{s}{\sigma(s)}$ and $\dfrac{t}{\sigma(t)}$ are not roots of unity. Apply Proposition 2.3 to the unit equation (37), we have that there exists a positive integer c and a finite set $\mathscr{S}'$ (contained in $\bar{L}^*$) such that for every $(m,n) \in \mathcal{M}(k,\ell,\sigma)$ the identities

$$\left(\frac{s^m}{\sigma(s^m)}\right)^{p^c} = x_1^{p^i}x_2^{p^j};\ \left(\frac{-u_{m,n,\sigma}t^n}{\sigma(s^m)}\right)^{p^c} = y_1^{p^i}y_2^{p^j};\ \left(\frac{u_{m,n,\sigma}\sigma(t^n)}{\sigma(s^m)}\right)^{p^c} = z_1^{p^i}z_2^{p^j} \tag{38}$$

hold for some $x_1,\dots,z_2 \in \mathscr{S}'$ and some $i,j \in \mathbb{N}_0$. Note that the last two equations of (38) implies that $\left(\dfrac{t^n}{\sigma(t^n)}\right)^{p^c}$ also has the form $w_1^{p^i}w_2^{p^j}$ where w_1 and w_2 belong to a finite set. Let $\tilde{G}$ be the group generated by this finite set, the set $\mathscr{S}'$, and the group G. Since $\dfrac{s}{\sigma(s)}$ and $\dfrac{t}{\sigma(t)}$ are non-torsion, using a basis of the free group $\tilde{G}/\tilde{G}_{\mathrm{tor}}$ to compare exponents as in the proof of Proposition 2.3, we have

that there exist finitely many quadruples $\mathbf{a}_h = (a_{h1}, a_{h2}, a_{h3}, a_{h4}) \in \mathbb{Q}^4$ for $h \in I$ such that $\mathscr{M}(k, \ell, \sigma)$ is contained in

$$\bigcup_{h \in I} F(p; a_{h1}, a_{h2}, a_{h3}, a_{h4})$$

where (recall Definition 1.8) $F(p; a_{h1}, \ldots, a_{h4}) = \{(a_{h1}p^i + a_{h2}p^j, a_{h3}p^i + a_{h4}p^j) : i, j \in \mathbb{N}_0\}$. This finishes the proof of Theorem 1.10.

5. An addendum to Theorem 1.10

For the sake of completeness, we briefly discuss Problem (B) under the condition that $\{s^n, t^n : n \in \mathbb{N}\} \cap \mathcal{O} \neq \emptyset$. The problem in this case becomes much easier and we model this section based on [Ngu15, Section 5] with appropriate modification for positive characteristic. Write $\mathcal{M} := \mathcal{M}(\mathcal{O}, s, t)$. For $\alpha, \beta \in \mathbb{N}$, let $A(\alpha, \beta)$ denote the arithmetic progression $\{k\alpha + \beta : k \in \mathbb{N}_0\}$. We may assume $t^f \in \mathcal{O}$ and consider two cases.

5.1. **The case $s^e \notin \mathcal{O}$.** For $1 \leq \ell \leq f$, let $\mathcal{M}(\cdot, \ell) := \{(m, n) \in \mathcal{M}(\mathcal{O}, s, t) : n \equiv \ell \bmod f\}$. Note that $\mathcal{M}(\cdot, f) = \emptyset$ since $K(s^e) \neq K$. We have:

Proposition 5.1. *The following results hold.*

(a) *For each $\ell \in \{1, \ldots, f-1\}$, $\pi_1(\mathcal{M}(\cdot, \ell))$ is a finite union of Frobenius subsets of $\mathbb{N}$.*
(b) *If $t^f \notin \mathcal{O}^*$ then $\mathcal{M}$ is a finite union of Frobenius subsets of $\mathbb{N}^2$.*
(c) *Assume $t^f \in \mathcal{O}^*$ and let $\ell \in \{1, \ldots, f-1\}$. Then $\mathcal{M}(\cdot, \ell) = \pi_1(\mathcal{M}(\cdot, \ell)) \times A(f, \ell)$.*

Proof. The same arguments in the proof of Proposition 4.7 can be used to prove part (a).

For part (b), note that $\pi_1(\mathcal{M})$ is a finite union of Frobenius subsets of $\mathbb{N}$ due to part (a). For any $m \in \pi_1(\mathcal{M})$, we prove that the set

$$\mathcal{M}_1(m) := \{n \in \mathbb{N} : (m, n) \in \mathcal{M}_1(m)\}$$

has at most $f - 1$ elements. Once this is done, we can use the same arguments as in the first case of the proof of Proposition 4.4. It suffices to show that for any $\ell \in \{1, \ldots, f-1\}$, there is at most one $n \in \mathbb{N}$ such that $(m, n) \in \mathcal{M}$ and $n \equiv \ell \bmod f$. Assume there are two such elements, namely $n_1 < n_2$. Write $n_1 = \tilde{n}_1 f + \ell$ and $n_2 = \tilde{n}_2 f + \ell$. Pick $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma \notin \mathrm{Gal}(L/K(s^e))$, hence σ does not fix any power of s. As before, there are units $u_{m,n_1,\sigma}$ and $u_{m,n_2,\sigma}$ in $\mathcal{O}[s^m, \sigma(s^m)]$ such that:

$$0 \neq s^m - \sigma(s^m) = u_{m,n_1,\sigma}(t^{n_1} - \sigma(t^{n_1})) = u_{m,n_1,\sigma}t^{\tilde{n}_1 f}(t^\ell - \sigma(t^\ell));$$

$$0 \neq s^m - \sigma(s^m) = u_{m,n_2,\sigma}(t^{n_2} - \sigma(t^{n_2})) = u_{m,n_2,\sigma}t^{\tilde{n}_2 f}(t^\ell - \sigma(t^\ell)).$$

This implies $t^{(\tilde{n}_2 - \tilde{n}_1)f}$ is a unit. Hence $t^f \in \mathcal{O}^*$, contradiction. This proves part (b).

Part (c) follows from the fact that $\mathcal{O}[t^n] = \mathcal{O}[t^\ell]$ for every $n \in A(f, \ell)$ since $t^f \in \mathcal{O}^*$. □

5.2. **The case $s^e \in \mathcal{O}$.** This could be taken almost verbatim from [Ngu15, Subsection 5.2], so we will be brief. It suffices to describe the set $\mathcal{M}(k,\ell)$ for $1 \le k \le e$ and $1 \le \ell \le f$. It is immediate that $W(e,\ell) = W(k,f) = \emptyset$ if $\ell < f$ and $k < e$. On the other hand, $W(e,f) = e\mathbb{N} \times f\mathbb{N}$.

From now on, we study $W(k,\ell)$ under the assumption that $k < e$ and $\ell < f$. We also assume $K(s^k) = K(t^\ell)$, otherwise $W(k,\ell) = \emptyset$. By the same arguments in [Ngu15, pp. 15], we have that if there exist distinct $(m_1,n_1),(m_2,n_2) \in W(k,\ell)$ then:

$$\frac{s^{m_2-m_1}}{t^{n_2-n_1}} \in \mathcal{O}^*. \tag{39}$$

We have the following:

Proposition 5.2. *The following results hold.*

(a) *If both s and t are units (i.e. $s,t \in \mathcal{O}_L^*$) then $W(k,\ell)$ is either empty or has the form*
$$(k,\ell) + e\mathbb{N} \times f\mathbb{N}.$$
(b) *If s is a unit and t is not then $W(k,\ell)$ is empty. The similar statement holds when t is a unit and s is not.*
(c) *Assume that neither s nor t is a unit. If $W(k,\ell) \neq \emptyset$ then the following holds. There is a minimal pair $(M,N) \in \mathbb{N}^2$ satisfying $\frac{s^{eM}}{t^{fN}} \in \mathcal{O}^*$. For any two distinct pairs $(m_1,n_1),(m_2,n_2) \in W(k,\ell)$, we have $(m_2-m_1)(n_2-n_1) > 0$. Moreover, we have $\frac{m_2-m_1}{eM} = \frac{n_2-n_1}{fN}$ and it is an integer.*

Proof. This is proved as in the proof of [Ngu15, Proposition 5.2]. The only difference is that in our current setting, if $W(k,\ell) \neq \emptyset$ then it is infinite. In fact, let $q > 1$ be a power of p such that $q \equiv 1 \bmod ef$. We have that $(qm,qn) \in W(k,\ell)$ whenever $(m,n) \in W(k,\ell)$. This fact and Equation (39) imply part (b). □

From now on, we assume that neither s nor t is a unit, there is a minimal pair $(M,N) \in \mathbb{N}^2$ such that $\frac{s^{eM}}{t^{fN}} \in \mathcal{O}^*$, and $W(k,\ell) \neq \emptyset$. Part (c) of Proposition 5.2 implies that $W(k,\ell)$ has a minimal element $(\tilde{m},\tilde{n})$ and every $(m,n) \in W(k,\ell)$ has the form $(\tilde{m}+\delta eM, \tilde{n}+\delta fN)$ for some $\delta \in \mathbb{N}_0$. We can use exactly the same method in [Ngu15, pp.16–17] to find an upper bound for $(\tilde{m},\tilde{n})$ and to determine all such δ's.

References

[AB12] B. Adamczewski and J. P. Bell, *On the set of zero coefficients of algebraic power series*, Invent. Math. **187** (2012), 343–393.

[AV92] D. Abramovich and J. F. Voloch, *Toward a proof of the Mordell-Lang conjecture in characteristic p*, Int. Math. Res. Not. IMRN **1992** (1992), 103–115.

[BEG13] A. Bérczes, J.-H. Evertse, and K. Győry, *Multiply monogenic orders*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **12** (2013), 467–497.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[BH09] J. P. Bell and K. G. Hare, *On $\mathbb{Z}$-modules of algebraic integers*, Canad. J. Math. **61** (2009), 264–281.

[BH12] ———, *Corrigendum to "on $\mathbb{Z}$-modules of algebraic integers"*, Canad. J. Math. **64** (2012), 254–256.

[Der07] H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristics and finite automata*, Invent. Math. **168** (2007), 175–224.

[DM12] H. Derksen and D. Masser, *Linear equations over multiplicative groups, recurrences, and mixing I*, Proc. Lond. Math. Soc. (3) **104** (2012), 1045–1083.

[EG85] J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358** (1985), 6–19.

[EG15] ———, *Unit Equations in Diophantine Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 146, Cambridge University Press, Cambridge, 2015.

[ESS02] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), 807–836.

[Ghi08] D. Ghioca, *The isotrivial case in the Mordell-Lang theorem*, Trans. Amer. Math. Soc. **360** (2008), 3839–3856.

[Győ84] K. Győry, *Effective finiteness theorem for polynomials with given discriminant and integral elements with discriminant over finitely generated domains*, J. Reine Angew. Math. **346** (1984), 54–100.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer, New York, 1977.

[Hru96] E. Hrushovski, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc. **9** (1996), 667–690.

[Mas04] D. Masser, *Mixing and linear equations over groups in positive characteristics*, Israel J. Math. **142** (2004), 189–204.

[MS04] R. Moosa and T. Scanlon, *f-structures and integral points on semiabelian varieties over finite fields*, Amer. J. Math. **126** (2004), 473–522.

[Neu99] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer-Verlag, 1999, Translated from the German by N. Schappacher.

[Ngu15] K. D. Nguyen, *On modules of integral elements over finitely generated domains*, To appear in Trans. Amer. Math. Soc. arXiv:1412.2868, 2015.

[Roq58] P. Roquette, *Einheiten und Divisorenklassen in endlich erzeugbaren Körpern*, Jber. Deutsch. Math. Verein **60** (1958), 1–21.

[Vol98] J. F. Voloch, *The equation $ax+by=1$ in characteristic p*, J. Number Theory **73** (1998), 195–200.

Jason P. Bell, University of Waterloo, Department of Pure Mathematics, Waterloo, Ontario, Canada N2L 3G1

E-mail address: jpbell@uwaterloo.ca

Khoa D. Nguyen, Department of Mathematics, University of British Columbia, And Pacific Institute for The Mathematical Sciences, Vancouver, BC V6T 1Z2, Canada

E-mail address: dknguyen@math.ubc.ca

URL: www.math.ubc.ca/~dknguyen